

Senate Finance Committee

*Senator Pamela Beidle, Chair
Senator Antonio Hayes, Vice-Chair*

Wednesday, January 22, 2025

Agenda

3:00 p.m.

Consumer's Right to Repair Motor Vehicles

- ***Safelite Group***

Bryson F. Popham, P.A., Lobbyist, Safelite Group

Michael A. Moné, BSPHarm, JD, Principal, Michael A. Mone & Associates

Tom Tucker, Assistant Vice President, Legislative Affairs, Safelite Group

Christopher Allen, Senior Corporate Counsel, Safelite Group

- ***Alliance for Automotive Innovation***

Wayne Weikel, Vice President, State Affairs

**Opening Statement by Tom Tucker
AVP, Legislative Affairs
Safelite Group, Inc.
January 22, 2025**

Chair Beidle and members of the Committee:

Good afternoon. My name is Tom Tucker, Assistant Vice President, Legislative Affairs for Safelite Group Inc. Safelite is the leading provider of automotive glass repair, replacement, and recalibrations services, along with insurance claims management in the United States. Safelite operates in all fifty states and is part of Belron International, the world's largest vehicle glass repair, replacement and recalibration company operating across thirty-eight countries worldwide and employing more than 25,000 people.

Thank you for convening this briefing and for the opportunity to speak with the committee regarding the issue of **Consumer's Rights in the Repair of Motor Vehicles**. This is an emerging issue that poses real questions about the future of auto repair and what rights does the consumer have with vehicles they own, operate, and insure.

A modern vehicle contains a vast amount of software, with estimates suggesting around 100-150 million lines of code and 25GB an hour of data flowing through its systems. There are over 1,500 wires totaling over 5,000 meters (three miles) in length. Autonomous vehicles will require even more code, potentially exceeding 300 and 500 million lines of code. This highlights the growing reliance on software within the automotive industry.

To put this into perspective:

- **The Hubble Space Telescope has two million lines of code.**
- **Modern PC operating systems typically have between twenty and fifty million lines of code.**

This surge in code complexity underscores the importance of software in the automotive industry. Modern cars are essentially computers on wheels, with their software and electronics playing a crucial role in every aspect of their operation. Therefore, who repairs these vehicles and how they are repaired becomes an important consideration.

The Right to Repair movement is here and has gained significant traction, with numerous states actively considering or enacting legislation related to it. At least forty states have introduced some form of Right to Repair legislation, demonstrating widespread interest in the topic since 2020. The movement incorporates a wide range of products, including consumer electronics, farm equipment, medical devices, automotive and more.

The core aim of Right to Repair laws is to give individuals and independent repair shops the legal right to access service information, replacement parts, and software tools to fix their personal property or to authorize access for the repairers of their choice.

Several states have enacted or are considering comprehensive Right to Repair laws, including California, Colorado, Massachusetts, Maine, Minnesota, and New York, among others. Currently, there are over twenty-five bills establishing the right to repair consumer items introduced in state legislatures across the country.

Some manufacturers and industry groups have voiced concerns about the potential impact of Right to Repair legislation on safety, intellectual property, and cyber security. While federal efforts to pass Right to Repair laws have been less successful, the movement continues to gain momentum at the state level.

In Massachusetts, an automotive right to repair ballot initiative overwhelmingly passed in 2020 and a similar ballot initiative passed in Maine in 2023. Those measures require the vehicle manufacturers to provide motor vehicle owners and authorized independent repair shops with all parts, tools, software, and other components necessary to complete a full repair of a vehicle. **(See Attachment A)**

The issue of the right to repair is an issue that should be studied carefully to ensure access to vehicle data, cybersecurity, and repairs are done properly according to the manufacturer's specifications.

The industry has been governed by an automotive right to repair MOU (Memorandum of Understanding) since 2013. **(See Attachment B)** The MOU, signed by automakers and aftermarket groups aims to ensure that independent repair shops have access to the same diagnostic and repair information as dealerships. However, it's a voluntary pact, a handshake agreement.

Many will argue that the MOU is not strong enough and lacks enforcement authority. It is also not legally binding and relies on automakers' voluntary compliance. In 2023, a new MOU was signed, not by a wide range of stakeholders, but rather with a small group of repairers aligned with the automakers. **(See Attachment C)**

The automakers view the MOU as a positive development, but its effectiveness hinges on automakers' commitment to its principles and the future adoption of enforceable regulations to ensure its long-term success.

Last year Massachusetts Senator Elizabeth Warren and Missouri Senator Josh Harley jointly penned a letter to the vehicle manufacturers criticizing their opposition to federal right to repair legislation while simultaneously selling consumer data themselves. **(See Attachment D)**

The auto makers claim that giving third-party access to what should be proprietary manufacturer data opens up cybersecurity and privacy risks. However, vehicle manufacturers routinely share sensitive vehicle and owner information with insurance companies and other third parties. At least thirty-seven car companies have been identified for monetizing the vehicle data they claim have privacy risks. **(See Attachment E)**

If the MOU is working effectively, why are repairers fighting for right to repair legislation and why are the manufacturers spending millions of dollars to oppose these efforts.

Let me pose this hypothetical question to you. Since the vehicle manufacturers oppose right to repair legislative efforts and unequivocally claim that the MOU is effective, would the manufacturers support allowing the consumer to sign a MOU when purchasing a new vehicle rather than a signed contract that has the force of law, penalties, and enforcement mechanisms if the consumer defaults? Shouldn't the consumer have those same legal protections with regard to the data generated by their vehicles?

Last year, when we began conversations with Maryland elected officials, we were referred to the Attorney General's office, as that office governs repair issues in the state. In our discussions, these specific questions were posed by the Attorney General's Office:

- What effect or connectivity is there between the right to repair initiative and the recently enacted data privacy law?
- Should repair data be considered personal data?
- Who owns the data in the vehicle?

These are legitimate questions for this committee to consider and the answers have far-reaching implications and consequences. Maryland consumers, repairers and the public should have clear guidance on who is authorized to access repair data. Therefore, we are requesting the committee to conduct a study to sort out these important questions.

We hope you see this is a logical approach to addressing this issue. Thank you for your time and consideration and I would be delighted to answer any questions from the committee on this issue.

ATTACHMENT A

AARON M. FREY
ATTORNEY GENERAL



TEL: (207) 626-8800
TTY USERS CALL MAINE RELAY 711

STATE OF MAINE
OFFICE OF THE ATTORNEY GENERAL
6 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0006

REGIONAL OFFICES
84 HARLOW ST. 2ND FLOOR
BANGOR, MAINE 04401
TEL: (207) 941-3070
FAX: (207) 941-3075

125 PRESUMPCOT ST., STE. 26
PORTLAND, MAINE 04103
TEL: (207) 822-0260
FAX: (207) 822-0259

14 ACCESS HIGHWAY, STE. 1
CARIBOU, MAINE 04736
TEL: (207) 496-3792
FAX: (207) 496-3291

NOTICE TO MAINE DEALERS

Under Maine law, 29-A M.R.S.A. § 1810, vehicle owners have the right to access their vehicle's mechanical data through a mobile device and to authorize an independent repair facility to access the vehicle's mechanical data to diagnose, repair, and maintain the vehicle. As of January 5, 2025, manufacturers of motor vehicles sold in Maine, including commercial motor vehicles and heavy-duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that use a telematics system, are required to equip vehicles sold in Maine with an inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models.

As required by Maine law (29-A M.R.S.A. § 1811), the Attorney General has established for prospective motor vehicle owners the accompanying Maine Motor Vehicle Telematics System Notice. Please note that the notice form provides for the prospective motor vehicle owner's signature certifying that the prospective owner has read the telematics system notice.

DEALER OBLIGATIONS: When selling or leasing motor vehicles containing a telematics system, a dealer as defined in Title 29-A, section 851, subsection 2 and a new vehicle dealer as defined in section 851, subsection 9 shall provide the telematics system notice under subsection 1 to the prospective owner, obtain the prospective owner's signed certification that the prospective owner has read the notice and provide a copy of the signed notice to the prospective owner.

ATTACHMENT B



AUTO ALLIANCE
DRIVING INNOVATION®

GlobalAutomakers 

AAIA®
Automotive Aftermarket
Industry Association



MEMORANDUM of UNDERSTANDING

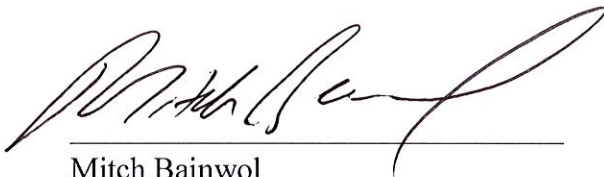
The Automotive Aftermarket Industry Association (“AAIA”), Coalition for Auto Repair Equality (“CARE”), Alliance of Automobile Manufacturers (“Alliance”) and Association of Global Automakers (“Global Automakers”) (“the Original Parties”) enter into this Memorandum of Understanding (MOU) on this Fifteenth (15th) day of January, 2014 and voluntarily agree as follows:

1. The Original Parties fully support this MOU and attached “Right to Repair” (R2R) agreement (“R2R Agreement”). Automobile manufacturer members of the Alliance and Global Automakers indicate their individual company’s agreement to comply with the MOU and R2R Agreement in all fifty (50) States and the District of Columbia through their individual letters of endorsement.
2. Until such time as the provisions of Section 2(c)(i) (common interface device) of the R2R Agreement have been fully implemented, with respect to model year 2018 and newer vehicles, for two years or January 2, 2019, whichever is earlier, and provided the OEMs comply with the MOU during this period, CARE and AAIA agree to continue to work with other Original Parties to fully implement the MOU and to oppose and not to fund or otherwise support, directly or indirectly, any new state R2R legislation.
3. The Original Parties agree to work to strongly encourage any new entrants to the U.S. automotive market or to R2R issues to become signatories to the MOU.
4. The Original Parties agree to work together to resolve any future or related R2R issues that might otherwise be the subject of state legislation and, subject to the mutual consent of the Original parties, amend the MOU and R2R Agreement to include these additional matters.
5. Once the Original Parties have signed on to the MOU, additional parties may join but any amendments or revisions to the terms of the MOU and R2R Agreement, triggered by admission of additional participants, shall require consent of the Original Parties.
6. The Original Parties agree to meet as needed and at least semi-annually, to assess how the MOU is operating, address operational concerns and discuss any other matters relevant to R2R or the MOU or future amendments or parties to the MOU. In the event that one of

the Original Parties concludes that, due to changed circumstances, the MOU or R2R Agreement may no longer be viable, that party shall, upon thirty (30) days written notice to the other three Original Parties, call a meeting to discuss the need for the MOU and R2R Agreement to continue.

7. The Original Parties agree that should a state(s) pass a law relating to issues covered by this MOU and R2R Agreement, after the effective date of the MOU and R2R Agreement, any automobile manufacturer member of the Alliance and Global Automakers may elect to withdraw its letter of endorsement for the MOU and R2R Agreement partially or entirely for the impacted state(s).

Signed on this 15th day of January, 2014:



Mitch Bainwol
President & CEO
Alliance of Automobile Manufacturers



Michael Stanton
President & CEO
Association of Global Automakers



Kathleen Schmatz
President & CEO
Automotive Aftermarket Industry Association



Ray Pohlman
President
Coalition for Auto Repair Equality

R2R AGREEMENT

Section 1. As used in this agreement, the following words shall, unless the context clearly indicates otherwise, have the following meanings:

“Dealer”, any person or business who, in the ordinary course of its business, is engaged in the business of selling or leasing new motor vehicles to consumers or other end users pursuant to a franchise agreement and who has obtained a license, as required under applicable law, and is engaged in the diagnosis, service, maintenance or repair of motor vehicles or motor vehicle engines pursuant to said franchise agreement.

“Franchise agreement”, a written arrangement for a definite or indefinite period in which a manufacturer or distributor grants to a motor vehicle dealer a license to use a trade name, service mark or related characteristic and in which there is a community of interest in the marketing of new motor vehicles or services related thereto at wholesale, retail, leasing or otherwise.

“Fair and Reasonable Terms” Provided that nothing in this MOU and R2R Agreement precludes an automaker and an owner or independent repair shop who is subject to the agreement from agreeing to the sale of information and tools on any other terms on which they agree, in determining whether a price is on “fair and reasonable terms,” consideration may be given to relevant factors, including, but not limited to, the following:

- (i) The net cost to the manufacturer’s franchised dealerships for similar information obtained from manufacturers, less any discounts, rebates, or other incentive programs.
- (ii) The cost to the manufacturer for preparing and distributing the information, excluding any research and development costs incurred in designing and implementing, upgrading or altering the onboard computer and its software or any other vehicle part or component. Amortized capital costs for the preparation and distribution of the information may be included.
- (iii) The price charged by other manufacturers for similar information.
- (iv) The price charged by manufacturers for similar information prior to the launch of manufacturer web sites.
- (v) The ability of aftermarket technicians or shops to afford the information.
- (vi) The means by which the information is distributed.
- (vii) The extent to which the information is used, which includes the number of users, and frequency, duration, and volume of use.
- (viii) Inflation.

“Immobilizer system”, an electronic device designed for the sole purpose of preventing the theft of a motor vehicle by preventing the motor vehicle in which it is installed from starting without the correct activation or authorization code.

"Independent repair facility", a person or business that is not affiliated with a manufacturer or manufacturer's authorized dealer of motor vehicles, which is engaged in the diagnosis, service, maintenance or repair of motor vehicles or motor vehicle engines;

"Manufacturer", any person or business engaged in the business of manufacturing or assembling new motor vehicles.

"Dispute Resolution Panel (DRP)", a 5-person panel established by the Original Parties comprised of the following: one Alliance representative, Alliance member or Alliance designee, one Global Automakers representative, Global Automakers' manufacturer member or Global Automakers designee, two representatives of the independent vehicle repair industry to be selected and mutually agreed upon by AAIA and CARE, and one DRP Chair. The DRP Chair shall be an independent professional mediator with no affiliation to any of the Original Parties, shall be selected by unanimous consent of the Original Parties and shall be funded in equal amounts by each of the Original Parties. The Original Parties shall, at one of the two annual meetings, have an opportunity to revisit their respective representative or ask the Original Parties to revisit the person acting as DRP Chair.

"Motor vehicle", any vehicle that is designed for transporting persons or property on a street or highway and that is certified by the manufacturer under all applicable federal safety and emissions standards and requirements for distribution and sale in the United States, but excluding (i) a motorcycle; (ii) a vehicle with a gross vehicle weight over 14,000 pounds; or (iii) a recreational vehicle or an auto home equipped for habitation.

"Owner", a person or business who owns or leases a registered motor vehicle.

"Trade secret", anything, tangible or intangible or electronically stored or kept, which constitutes, represents, evidences or records intellectual property including secret or confidentially held designs, processes, procedures, formulas, inventions, or improvements, or secret or confidentially held scientific, technical, merchandising, production, financial, business or management information, or anything within the definition of 18 U.S.C. § 1839(3).

Section 2.

(2)(a). Except as provided in subsection (2)(e), for Model Year 2002 motor vehicles and thereafter, a manufacturer of motor vehicles sold in United States shall make available for purchase by owners of motor vehicles manufactured by such manufacturer and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that such manufacturer makes available to its dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system. All content in any such manufacturer's repair information system shall be made available to owners and to independent repair facilities in the same form and manner and to the same extent as is made available to dealers utilizing such diagnostic and repair information system. Each manufacturer shall provide access to such manufacturer's diagnostic and repair information system for purchase by owners and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.

(2)(b)(i) For Model Year 2002 motor vehicles and thereafter, each manufacturer of motor vehicles sold in the United States shall make available for purchase by owners and independent repair facilities all diagnostic repair tools incorporating the same diagnostic, repair and wireless capabilities that such manufacturer makes available to its dealers. Such tools shall incorporate the same functional repair capabilities that such manufacturer makes available to dealers. Each manufacturer shall offer such tools for sale to owners and to independent repair facilities upon fair and reasonable terms.

(ii) Each manufacturer shall provide diagnostic repair information to each aftermarket scan tool company and each third party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and third party service information publications and systems. Once a manufacturer makes such information available pursuant to this section, the manufacturer will have fully satisfied its obligations under this section and thereafter not be responsible for the content and functionality of aftermarket diagnostic tools or service information systems.

(2)(c)(i) Commencing in Model Year 2018, except as provided in subsection (2)(e), manufacturers of motor vehicles sold in the United States shall provide access to their onboard diagnostic and repair information system, as required under this section, using an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer and:

(a) a non-proprietary vehicle interface device that complies with the Society of Automotive Engineers SAE J2534, the International Standards Organizations ISO 22900 or any successor to SAE J2534 or ISO 22900 as may be accepted or published by the Society of Automotive Engineers or the International Standards Organizations; or,

(b) an on-board diagnostic and repair information system integrated and entirely self-contained within the vehicle including, but not limited to, service information systems integrated into an onboard display, or

(c) a system that provides direct access to on-board diagnostic and repair information through a non-proprietary vehicle interface such as Ethernet, Universal Serial Bus or Digital Versatile Disc. Each manufacturer shall provide access to the same on-board diagnostic and repair information available to their dealers, including technical updates to such on-board systems, through such non-proprietary interfaces as referenced in this paragraph. Nothing in this agreement shall be construed to require a dealer to use the non-proprietary vehicle interface (i.e., SAE J2534 or ISO 22900 vehicle interface device) specified in this subsection, nor shall this agreement be construed to prohibit a manufacturer from developing a proprietary vehicle diagnostic and reprogramming device, provided that the manufacturer also complies with Section 2(c)(i) and the manufacturer also makes this device available to independent repair facilities upon fair and reasonable terms, and otherwise complies with Section 2(a).

(2)(c)(ii) No manufacturer shall be prohibited from making proprietary tools available to dealers if such tools are for a specific specialized diagnostic or repair procedure developed for

the sole purpose of a customer service campaign meeting the requirements set out in 49 CFR 579.5, or performance of a specific technical service bulletin or recall after the vehicle was produced, and where original vehicle design was not originally intended for direct interface through the non-proprietary interface set out in (2)(c)(i). Provision of such proprietary tools under this paragraph shall not constitute a violation of this agreement even if such tools provide functions not available through the interface set forth in (2)(c)(i), provided such proprietary tools are also available to the aftermarket upon fair and reasonable terms. Nothing in this subsection (2)(c)(ii) authorizes manufacturers to exclusively develop proprietary tools, without a non-proprietary equivalent as set forth in (2)(c)(i), for diagnostic or repair procedures that fall outside the provisions of (2)(c)(ii) or to otherwise operate in a manner inconsistent with the requirements of (2)(c)(i).

(2)(d) Manufacturers of motor vehicles sold in the United States may exclude diagnostic, service and repair information necessary to reset an immobilizer system or security-related electronic modules from information provided to owners and independent repair facilities. If excluded under this paragraph, the information necessary to reset an immobilizer system or security-related electronic modules shall be obtained by owners and independent repair facilities through the secure data release model system as currently used by the National Automotive Service Task Force or other known, reliable and accepted systems.

(2)(e) With the exception of telematics diagnostic and repair information that is provided to dealers, necessary to diagnose and repair a customer's vehicle, and not otherwise available to an independent repair facility via the tools specified in 2(c)(i) above, nothing in this agreement shall apply to telematics services or any other remote or information service, diagnostic or otherwise, delivered to or derived from the vehicle by mobile communications; provided, however, that nothing in this agreement shall be construed to abrogate a telematics services or other contract that exists between a manufacturer or service provider, a motor vehicle owner, and/or a dealer. For purposes of this agreement, telematics services include but are not limited to automatic airbag deployment and crash notification, remote diagnostics, navigation, stolen vehicle location, remote door unlock, transmitting emergency and vehicle location information to public safety answering points as well as any other service integrating vehicle location technology and wireless communications. Nothing in this agreement shall require a manufacturer or a dealer to disclose to any person the identity of existing customers or customer lists.

Section 3. Nothing in this agreement shall be construed to require a manufacturer to divulge a trade secret.

Section 4. Notwithstanding any general or special law or any rule or regulation to the contrary, no provision in this agreement shall be read, interpreted or construed to abrogate, interfere with, contradict or alter the terms of any franchise agreement executed and in force between a dealer and a manufacturer including, but not limited to, the performance or provision of warranty or recall repair work by a dealer on behalf of a manufacturer pursuant to such franchise agreement.

Section 5. Nothing in this agreement shall be construed to require manufacturers or dealers to provide an owner or independent repair facility access to non-diagnostic and repair information

provided by a manufacturer to a dealer, or by a dealer to a manufacturer pursuant to the terms of a franchise agreement.

Section 6. If an independent repair facility or owner believes that a manufacturer has failed to provide the information or tool required by this MOU, he may challenge the manufacturer's actions by first notifying the manufacturer in writing. The manufacturer has thirty (30) days from the time it receives the reasonably clear and specific complaint to cure the failure, unless the parties otherwise agree. If the complainant is not satisfied, he has thirty (30) days to appeal the manufacturer's decision to the DRP. The DRP shall be convened by the Chair within thirty (30) days of receipt of the appeal of the manufacturer's decision. The DRP will attempt to reach agreement between the parties. If unsuccessful, the DRP shall convene and issue its decision. The decision must be issued within 30 days of receipt of the appeal of the manufacturer's decision, unless otherwise agreed to by the parties. The DRP decision shall be disseminated to the complainant, the manufacturer, and the Original Parties. If the manufacturer and complainant still cannot reach agreement, the complainant may take whatever legal measures are available to it.

ATTACHMENT C



Automotive Repair Data Sharing Commitment

This commitment was created with one group of people in mind: vehicle owners. It recognizes and reaffirms the belief that consumers should have access to safe and proper repairs throughout a vehicle's lifecycle.

The parties commit to ensure consumer choice in vehicle repair decisions and support the independent repair community as provided below and as outlined in the existing 2014 Memorandum of Understanding:

Access to diagnostic and repair information – There shall be available for purchase by owners of motor vehicles and by independent repair facilities on fair and reasonable terms the same diagnostic and repair information, including service manuals and technical repair updates, that a manufacturer makes available to its authorized dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible repair information system.

Access to vehicle systems – There shall be available access to vehicle diagnostic systems through (i) a non-proprietary vehicle interface device that complies with the Society of Automotive Engineers standard J2534, commonly referred to as SAE J2534, the International Organization for Standardization standard 22900, commonly referred to as ISO 22900 or any successor to SAE J2534 or ISO 22900 as may be accepted or published by the Society of Automotive Engineers or the International Organization for Standardization; (ii) an onboard diagnostic and repair data system integrated and entirely self-contained within the vehicle, including, but not limited to, diagnostic or service information systems integrated into an onboard display; or (iii) a system that provides direct access to onboard diagnostic and repair data through a non-proprietary vehicle interface, such as ethernet, universal serial bus or digital versatile disc; provided that each manufacturer provides access to the same onboard diagnostic and repair data and functions available to their dealers, including technical updates to such onboard systems, through such non-proprietary interfaces as referenced in this paragraph.

Alternate Fueled Vehicles – Just as is the case for traditional internal combustion vehicles, access to vehicle diagnostic data and to vehicle systems for diagnostic and repair purposes shall be available for purchase by vehicle owners and by independent repair facilities on fair and reasonable terms for alternately fueled vehicles. This commitment applies to all vehicle technologies regardless of powertrain, including gasoline, diesel, fuel cell, electric battery, hybrid, and plug-in hybrid electric powertrains.

Telematics – Telematics systems shall not be used to circumvent the commitments made in this commitment to provide independent repair facilities with access to vehicle diagnostic data. To the extent that specific telematic diagnostic and repair data is needed to complete a repair, and also provided to an automaker’s authorized dealers, the automaker shall make such information available to vehicle owners and independent repair facilities, if it is not otherwise available through a tool or third-party service information provider. This does not apply to any telematics data beyond what is necessary to diagnose and repair a vehicle.

Access to tools – There shall be made available for purchase by owners of motor vehicles and by independent repair facilities diagnostic repair tools incorporating the same functional capabilities that a manufacturer makes available to its authorized dealers.

Fair and Reasonable Terms – There shall be access to diagnostic and repair information and tools on fair and reasonable terms, consistent with U.S. Environmental Protection Agency, California Air Resources Board, and Massachusetts statutory requirements.

Support of Third-Party Tool Manufacturers – Diagnostic and repair information shall be made available to each third-party tool manufacturer and each third-party service information provider with whom a manufacturer has appropriate licensing, contractual, or confidentiality commitment for the sole purpose of building diagnostic tools and third-party service information publications and systems.

Trade secret protections – Nothing in this commitment shall be construed to require a manufacturer to divulge a trade secret.

Education – The parties shall develop a plan to educate both mechanical and collision repair facilities on the avenues by which they can access repair information, including directly through manufacturer repair websites, on www.oem1stop.com, or by accessing third-party tool and data service providers, among others.

Training – The parties shall review existing training options for both mechanical and collision repair facilities and work to ensure repairers have access to the latest training opportunities.

Working Together to Address Any Identified Gaps

As a complement to the existing process for resolving disputes involving the availability of diagnostic and repair information from specific manufacturers established in the 2014 MOU, the parties commit to establish a Vehicle Data Access Panel (VDAP) to identify issues a party may have with respect to the availability of diagnostic data and repair information as pledged in this commitment and collaborate on potential solutions where feasible. The VDAP shall be comprised of representatives from Automotive Service Association, Society of Collision Repair Specialists and Alliance for Automotive Innovation, and shall meet, at a minimum, biannually.

Periodic Review to Ensure Continued Relevancy

In recognition of this industry's dynamic marketplace, the parties commit to review this commitment annually and update, if appropriate. To that end, the parties shall establish a Data Access Working Group to consider any technological advancements that may alter the vehicle repair marketplace. The size and membership of this Working Group shall be established by the parties and can be altered at any time with the commitment of the signing parties.

Cooperation and Advocacy

Federal legislation – The parties commit to working together in support of federal legislation to codify the various provisions of this commitment, ensuring consumer choice in vehicle repair across the country. The parties also commit to working together against any legislation that is in direct conflict with the tenets of this document.

Federal regulations – The parties commit to working together in support of a petition to the Environmental Protection Agency to ensure reparability of electric vehicles by requiring standardized data communication protocols from OBDII-type connectors on all battery electric, plug-in hybrid, hybrid, and fuel cell vehicles model year 2026 and beyond in alignment with California's Advanced Clean Cars II regulation.

State legislation – The parties commit to working together against any legislation that is in conflict with the tenets of this commitment. Engagement on state legislation not in conflict with the tenets of this commitment shall be evaluated on its merits and subject to the commitment of the parties.

Signing Parties

Automotive Service Association (ASA)

ASA is the largest and oldest national organization committed to protecting the automotive repair industry with ONE VOICE. Our members own and operate automotive mechanical and collision repair facilities responsible for the majority of all, post warranty, repair services in the United States. ASA advocates for the interests of its members and their customers in Washington, D.C. The education, resources, and services ASA provides empowers its members in all 50 states to remain trusted stewards of mobility in their communities. www.ASAShop.org

Society of Collision Repair Specialists (SCRS)

Through our direct members and affiliate associations, SCRS proudly represents over 6,000 collision repair businesses and 58,500 specialized professionals who work to repair collision-damaged vehicles. Since 1982, SCRS has served as the largest national trade association solely dedicated to the hardworking collision repair facilities across North America. Since its formation, SCRS has provided repairers with an audible voice, and an extensive grassroots network of industry professionals who strive to better our trade. Additional information about SCRS including other news releases is available at the SCRS website. www.scrs.com

Alliance for Automotive Innovation

From the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers – Alliance for Automotive Innovation represents the full auto industry, a sector supporting 10 million American jobs and five percent of the economy. Active in Washington, D.C. and all 50 states, the association is committed to a cleaner, safer and smarter personal transportation future.

www.autosinnovate.org

Effective Date

This Commitment is effective immediately upon signed letter transmittal to Chairwoman Cantwell, Ranking Member Cruz, Chairwoman McMorris Rodgers, Ranking Member Pallone, Chairman Jordan, Ranking Member Nadler, Chairman Durbin, and Ranking Member Graham.

ATTACHMENT D
United States Senate

WASHINGTON, DC 20510

December 19, 2024

Jim D. Farley, Jr.
President and CEO
Ford Motor Company
P.O. Box 6248
Dearborn, MI 48126

Dear Mr. Farley:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

from the cars and software partnerships with large industry players to eliminate parts competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on connected devices, including cars, “exploit software vulnerabilities in embedded software

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Secure Repairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-ai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Ford to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Ford respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Ford receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Mary Barra
Chair and CEO
General Motors Company
P.O. BOX 33170
Detroit, MI 48232

Dear Mrs. Barra:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

from the cars and software partnerships with large industry players to eliminate parts competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on connected devices, including cars, “exploit software vulnerabilities in embedded software

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Secure Repairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-ai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge General Motors to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that General Motors respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did General Motors receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Kazuhiro Takizawa
President, CEO and Director
American Honda Motor Co., Inc.
1919 Torrance Boulevard
Torrance, CA 90501

Dear Mr. Takizawa:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmland/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

from the cars and software partnerships with large industry players to eliminate parts competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-pretial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on connected devices, including cars, “exploit software vulnerabilities in embedded software

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Secure Repairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-ai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Honda to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Honda respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Honda receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Randy Parker
CEO
Hyundai Motor America
P.O. Box 1430
Mesa, AZ 85211

Dear Mr. Parker:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

from the cars and software partnerships with large industry players to eliminate parts competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on connected devices, including cars, “exploit software vulnerabilities in embedded software

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Secure Repairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-ai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Hyundai to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Hyundai respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Hyundai receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Jérémie Papin
Chair
Nissan North America, Inc.
One Nissan Way
Franklin, TN 37067

Dear Mr. Papin:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

from the cars and software partnerships with large industry players to eliminate parts competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on connected devices, including cars, “exploit software vulnerabilities in embedded software

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Secure Repairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-ai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Nissan to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Nissan respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Nissan receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Antonio Filosa
COO
Stellantis North America
800 Chrysler Drive
Auburn Hills, MI 48326

Dear Mr. Filosa:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

“Right-to-repair,” which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been “leveraging new technological advantages gained through telematics from the cars and software partnerships with large industry players to eliminate parts

¹ U.S. Government Accountability Office, “Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice,” March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, “Massachusetts Voters Approve Ballot Question 1 Expanding ‘Right To Repair’ Law,” November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, “Missouri among states eyeing ‘right to repair’ laws for farm equipment,” February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, “Right to Repair,” <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, “Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair,” press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts->

connected devices, including cars, “exploit software vulnerabilities in embedded software produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

[testimony-sm.pdf](#).

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., SecureRepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Stellantis to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Stellantis respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Stellantis receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Tadashi “Tady” Yoshida
Chairman and CEO
Subaru of America, Inc.
One Subaru Drive
Camden, NJ 08103

Dear Mr. Yoshida:

We write regarding our concerns about automakers’ fierce opposition to nationwide efforts to secure car owners’ right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers’ hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

“Right-to-repair,” which refers to consumers’ ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been “leveraging new technological advantages gained through telematics from the cars and software partnerships with large industry players to eliminate parts

¹ U.S. Government Accountability Office, “Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice,” March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, “Massachusetts Voters Approve Ballot Question 1 Expanding ‘Right To Repair’ Law,” November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, “Missouri among states eyeing ‘right to repair’ laws for farm equipment,” February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, “Right to Repair,” <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, “Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair,” press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-pretial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts->

connected devices, including cars, “exploit software vulnerabilities in embedded software produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

[testimony-sm.pdf](#).

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., SecureRepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Subaru to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Subaru respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Subaru receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Elon Musk
CEO
Tesla, Inc.
1 Tesla Road
Austin, TX 78725

Dear Mr. Musk:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics from the cars and software partnerships with large industry players to eliminate parts

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2,

connected devices, including cars, “exploit software vulnerabilities in embedded software produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

<https://judiciary.house.gov/sites/evo-subsites/repUBLICans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., SecureRepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-pretial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Tesla to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Tesla respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Tesla receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Tetsuo “Ted” Ogawa
President and CEO
Toyota Motor North America, Inc.
P.O. Box 259001
Plano, TX 75025

Dear Mr. Ogawa:

We write regarding our concerns about automakers’ fierce opposition to nationwide efforts to secure car owners’ right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers’ hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

“Right-to-repair,” which refers to consumers’ ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been “leveraging new technological advantages gained through telematics from the cars and software partnerships with large industry players to eliminate parts

¹ U.S. Government Accountability Office, “Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice,” March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, “Massachusetts Voters Approve Ballot Question 1 Expanding ‘Right To Repair’ Law,” November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, “Missouri among states eyeing ‘right to repair’ laws for farm equipment,” February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, “Right to Repair,” <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, “Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair,” press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2,

connected devices, including cars, “exploit software vulnerabilities in embedded software produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

<https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., SecureRepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-pretial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Toyota to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Toyota respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Toyota receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

United States Senate

WASHINGTON, DC 20510

December 19, 2024

Kjell Gruner
President and CEO
Volkswagen Group of America, Inc.
1950 Opportunity Way
Reston, VA 20190

Dear Mr. Gruner:

We write regarding our concerns about automakers' fierce opposition to nationwide efforts to secure car owners' right to repair the vehicles they own in the way they choose. We are particularly disturbed by the automakers' hypocrisy with regard to data sharing. The industry has raised concerns about data sharing with independent repair shops to justify opposing right-to-repair, while earning profits from sharing large amounts of personal data with insurance companies.

"Right-to-repair," which refers to consumers' ability to decide who repairs their products,¹ is a foundational component of consumer choice. Robust right-to-repair protections are important to consumers, businesses, and the American agricultural industry. Passage of right-to-repair laws across the country reflects overwhelming consumer preference for right-to-repair protections, despite outsized spending by automakers and other original equipment manufacturers in opposition.² More than half of Americans say they do not believe consumers have enough choices when it comes to choosing where they will get something repaired, and 84% say they support a policy that would require manufacturers to make repair information and parts more accessible.³

Consumer protection experts have echoed these sentiments, finding that repair restrictions harm consumers by raising prices and preventing timely repairs.⁴ Empirical research indicates that car manufacturers have been "leveraging new technological advantages gained through telematics

¹ U.S. Government Accountability Office, "Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice," March 21, 2024, p. 1, <https://www.gao.gov/assets/d24106633.pdf>.

² See, e.g., CBS News, "Massachusetts Voters Approve Ballot Question 1 Expanding 'Right To Repair' Law," November 3, 2020, <https://www.cbsnews.com/boston/news/election-2020-results-massachusetts-question-1-right-to-repair/>; FOX 2 News, "Missouri among states eyeing 'right to repair' laws for farm equipment," February 13, 2023, <https://fox2now.com/news/missouri/11-states-eye-right-to-repair-laws-for-farmequipment/>; PIRG, "Right to Repair," <https://pirg.org/campaigns/right-to-repair/> (listing legislation passed in dozens of states to protect right-to-repair in farm equipment, consumer devices, power wheelchairs, home appliances, and other sectors).

³ Consumer Reports, "Consumer Reports Survey Finds Americans Overwhelmingly Support the Right to Repair," press release, February 28, 2022, https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-americans-overwhelmingly-support-the-right-to-repair/.

⁴ Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," May 2021, p. 38, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

from the cars and software partnerships with large industry players to eliminate parts competition.”⁵ Currently, consumers get approximately 70 percent of car parts and services from independent providers, and 30 percent from dealerships.⁶ This is because repairs by independent providers are cheaper: customers give independent repair shops good ratings on price (as well as overall satisfaction), while nearly all dealerships receive the worst possible rating for price.⁷ Overall, car owners appreciate independent repair shops for their “trustworthiness, reasonable prices, knowledgeable mechanics, and good reputation.”⁸ The ability for car owners to repair their vehicles without breaking the bank is particularly important given that Americans buy twice as many used cars as new ones.⁹

By barring the potential use of non-manufacturer replacement parts, such as salvaged parts at independent repair shops, auto manufacturers are able effectively to create product monopolies and inflate repair prices.¹⁰ As this limits options for repair, consumers face a slow and inconvenient process, often having to “surrender their cars . . . for days or weeks to get them fixed.”¹¹

Right-to-repair is crucial for independent repair shops and local economies. More than 80 percent of independent repair shops view data access as “the top issue for their business,” surpassing considerations like inflation and technician recruitment and retention, and more than 60 percent “experienced difficulty making routine repairs on a daily or weekly basis” because of automakers’ restrictions.¹² Restrictions currently cost independent repair shops \$3.1 billion each year,¹³ a figure poised to increase as car components become increasingly digital.

As the gatekeepers of vehicle parts, equipment, and data, automobile manufacturers have the power to place restrictions on the necessary tools and information for repairs, particularly as cars increasingly incorporate electronic components. This often leaves car owners with no other option than to have their vehicles serviced by official dealerships, entrenching auto manufacturers’ dominance and eliminating competition from independent repair shops.

⁵ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 40, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

⁶ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 12, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

⁷ Consumer Reports, “Car Owners Favor Independent Repair Shops,” Benjamin Preston, March 20, 2024, <https://www.consumerreports.org/cars/car-repair-shops/car-repair-shop-survey-chains-dealers-independents-a1071080370/>.

⁸ *Id.*

⁹ CAR Coalition, “White Paper on the Right to Equitable and Professional Auto Industry Repair (REPAIR) Act, H.R. 6570, 117th Congress,” September 2022, p. 11, <https://carcoalition.com/wp-content/uploads/2020/07/Repair-Act-white-paper-09-13-2022-1.pdf>.

¹⁰ *Id.*

¹¹ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Securepairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, p. 15, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aaai-pretrial_0.pdf.

¹² Auto Care Association, “Survey: 84% of Independent Repair Shops View Vehicle Data Access as Top Issue for Their Business,” April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

¹³ *Id.*

Automakers' Cybersecurity Concerns Are Specious

Auto manufacturers have routinely raised cybersecurity risks as an excuse for opposing right-to-repair, attempting to distract consumers from the fact that “vehicle repair and maintenance services from independent repair shops keeps the cost of service and repair down.”¹⁴ For example, the lobbying group representing automakers recently warned that the federal government should be “concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.”¹⁵ The head of digital policy at Europe’s similar lobbying group has said that “[o]pening the possibility for third parties to trigger safety-critical functions remotely is very concerning.”¹⁶ These cybersecurity concerns are often based on speculative future risks rather than facts. A study by the Federal Trade Commission (FTC) found no evidence to back up the cybersecurity arguments made by manufacturers to limit repair opportunities by independent repair shops, and “no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data.”¹⁷ According to the FTC, allowing independent repair shops to access diagnostic software and firmware patches, far from jeopardizing security, is consistent with the FTC’s data security guidance.¹⁸ Outside the United States, where automakers have attempted similar strategies to shut down independent repair, a German court just last month ruled against Mercedes-Benz that automakers should not use cybersecurity as an excuse to restrict data access to suppliers.¹⁹

Cybersecurity experts have forcefully pushed against manufacturers’ fearmongering. Security expert Paul Roberts testified before the House Judiciary Committee in July 2023 that “information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers.”²⁰ The vast majority of attacks on connected devices, including cars, “exploit software vulnerabilities in embedded software

¹⁴ VICE, “Auto Industry Has Spent \$25 Million Lobbying Against right-to-repair Ballot Measure,” Matthew Gault, September 29, 2020, <https://www.vice.com/en/article/z3ead3/auto-industry-has-spent-dollar25-million-lobbying-against-right-to-repair-ballot-measure>.

¹⁵ Alliance for Automotive Innovation, “Comments to BIS on Securing the ICTS Supply Chain for Connected Vehicles,” April 30, 2024, p. 10, <https://www.autosinnovate.org/posts/agency-comments/comments-bis-connected-car-anprm>.

¹⁶ Wall Street Journal, “Automakers and Suppliers Spar Over Car Data,” Catherine Stupp, October 24, 2023, <https://www.wsj.com/articles/automakers-and-suppliers-spar-over-car-data-a5e7dbaf>.

¹⁷ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission on Repair Restrictions Before The Judiciary Committee California State Senate,” April 11, 2023, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/P194400-Nixing-the-Fix-California-Senate-Judiciary-Committee-Testimony.pdf; Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, pp. 24-36, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁸ Federal Trade Commission, “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021, p. 31, https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

¹⁹ Wall Street Journal, “Courts Side With Auto Suppliers in Clash With Carmakers Over Vehicle Data Access,” Catherine Stupp, October 24, 2024, <https://www.wsj.com/articles/courts-side-with-auto-suppliers-in-clash-with-carmakers-over-vehicle-data-access-96871fdd>.

produced, managed and released by the manufacturer,” meaning that “it is the poor quality of deployed software and the poor state of device security – not the availability of diagnostic and repair tools and information – that fuels cyber attacks on connected devices.”²¹

Auto manufacturers’ opposition to right-to-repair on cybersecurity grounds is at odds with cybersecurity best practices, which have abandoned the practice of “security through obscurity,” recognizing that “secrecy isn’t the same as security.”²² A cybersecurity approach premised on exclusive access to data by car manufacturers is an example of security through obscurity, which “allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be identified and repaired, while increasing the likelihood that flaws can and will be exploited by evil-doers.”²³ Further, examples of cyberattacks on moving vehicles that have been utilized to scare policymakers into embracing car manufacturers’ positions have in fact historically “not depended on access to telematics data” of the kind at issue in right-to-repair proposals.²⁴ Car manufacturers should not hide behind a false dichotomy of cybersecurity and consumer choice in order to avoid their legal obligations to facilitate independent vehicle repair.

Auto Manufacturers Share Sensitive Consumer Data with Insurance Companies and Other Third Parties

Automakers’ own data practices show that their claims around cybersecurity derive from ulterior motives. While carmakers have been fighting tooth and nail against right-to-repair laws that would require them to share vehicle data with consumers and independent repairers, they have simultaneously been sharing large amounts of sensitive consumer data with insurance companies and other third parties for profit — often without clear consumer consent. In fact, some car companies use the threat of increased insurance costs to push consumers to opt into safe driving features, and then use those features to collect and sell the user data. A 2024 investigation revealed that automakers were selling user driving data, such as acceleration and brake patterns, to data brokers.²⁵ Lawmakers have specifically called out General Motors, Hyundai, and Honda for using deceptive tactics to collect customers’ driving data and then sell it to data brokers.²⁶ Through these practices, Hyundai was able to make over \$1 million.²⁷ This information on

²⁰ House Judiciary Committee, “Testimony of Paul Roberts, Founder of Secure Repairs, before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,” July 14, 2023, p. 2, <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/roberts-testimony-sm.pdf>.

²¹ *Id.*, p. 3.

²² Forbes, “Tilting Against Repair Law, NHTSA Endorses Security Through Obscurity,” Paul F. Roberts, June 21, 2023, <https://www.forbes.com/sites/paulfroberts/2023/06/21/tilting-against-repair-law-nhtsa-endorses-security-through-obscurity/?sh=1510e7e3428b>.

²³ Alliance for Automotive Innovation v. Maura Healey, Attorney General of the Commonwealth of Massachusetts, Case No. 1:20-cv-12090-DPW, Brief of iFixit, The Repair Association, U.S. PIRG Education Fund, Inc., Secure Repairs.org, The Electronic Frontier Foundation, and Professor Jonathan Askin as *Amici Curiae* in Support of Defendant, pp. 10-11, June 7, 2021, https://www.eff.org/files/2021/06/08/brief-ifixit-aa-ai-pretrial_0.pdf (internal citations omitted).

²⁴ *Id.*

²⁵ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁶ Boston Herald, “Markey calls for auto data probe,” July 28, 2024, <https://www.bostonherald.com/2024/07/28/markey-calls-for-auto-data-probe/>.

²⁷ *Id.*

driving patterns obtained by the data brokers was then sold to and used by auto insurers to vastly increase insurance prices.²⁸

At least 37 car companies have been identified as a part of the connected vehicle data industry that seeks to monetize such data,²⁹ but as vehicles become increasingly connected, automotive companies stand to gain greater incentive for collecting and monetizing this data themselves. It is estimated that there will be around 470 million connected vehicles on highways around the world by 2025 and each of these connected vehicles will produce roughly 25 gigabytes of data per hour.³⁰ This data is expected to be worth up to \$800 billion by 2030.³¹ As of 2022, data brokers such as LexisNexis have shared that they have access to “real-world driving behavior” from over 10 million vehicles.³² Those data brokers’ own marketing materials underscore the sensitive nature of the data that automakers sell, including:

- Last parking location,
- Current geolocation,
- Lock status,
- Ignition status,
- Data on the last trip taken,
- Mileage,
- Vehicle speed,
- Accident events,
- Crashes,
- Odometer status, and
- Use of seatbelts.³³

Despite the enormous amounts of data collection by car companies from consumers, few of these manufacturers comply with basic security standards.³⁴

²⁸ New York Times, “Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies,” Kashmir Hill, March, 11, 2024, <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

²⁹ The Markup, “Who Is Collecting Data from Your Car?,” Jon Keegan and Alfred Ng, July 27, 2022, <https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>.

³⁰ Netscribes, “The road to profitability: Why automotive data monetization is the next big thing,” Kanika Shukla, March 24, 2023, <https://www.netscribes.com/the-road-to-profitability-why-automotive-data-monetization-is-the-next-big-thing/>.

³¹ Capgemini, “Monetizing Vehicle Data: How to fulfill the promise,” September 2020, p. 5, https://s3.documentcloud.org/documents/22120767/capgeminiinvent_vehicledatamonetization_pov_sep2020.pdf.

³² LexisNexis Risk Solutions, “LexisNexis Telematics Exchange Celebrates 5-Year Anniversary,” press release, June 28, 2022, <https://risk.lexisnexis.com/about-us/press-room/press-release/20220628-telematics-exchange-5-year-anniversary>.

³³ Caruso Dataplace, “Developer Catalog,” <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>; High Mobility, “Auto API Data Categories,” <https://www.high-mobility.com/car-data>.

³⁴ Mozilla, “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,” Jen Caltrider, Misha Rykov, and Zoë MacDonald, September 6, 2023, <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

Conclusion

Right-to-repair laws support consumer choice and prevent automakers from using restrictive repair laws to their financial advantage. It is clear that the motivation behind automotive companies' avoidance of complying with right-to-repair laws is not due to a concern for consumer security or privacy, but instead a hypocritical, profit-driven reaction. This kind of anti-consumer, anti-repair practice must come to an end in all industries. Americans have a right to fix their own technology, farm equipment, and automobiles.

We urge Volkswagen to comply with all right-to-repair laws while protecting consumer privacy interests. We also ask that Volkswagen respond to the following questions by January 6, 2025:

1. How much in direct income and other benefits did Volkswagen receive from car repairs in each of the previous five years, including income derived from repairs at dealerships, authorized dealer networks, and other affiliated locations?
2. What user and driving data do your company's cars collect, and how frequently is this data collected?
3. How do you seek consent from drivers for data sharing?
 - a. What steps must car owners take to access their own data?
4. What user data does your company share with third parties? Please list the third parties with which your company shares data.
5. For each of the third parties listed in Question 4, please detail the specific data that is shared, and the revenue obtained from each data sharing agreement.
6. How does your company protect the data it collects from users?
7. What measures does your company take to protect user privacy, if any?
 - a. If your company de-identifies data it collects from users, how do you protect against the data being re-identified?
8. Please list all data breaches or other cybersecurity incidents involving your company or your company's vehicles in the last five years.
9. How much has your company spent lobbying against right-to-repair measures?
10. Please list the organizations or associations your company is part of that lobby against right-to-repair measures.

Sincerely,



Elizabeth Warren
United States Senator



Josh Hawley
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

ATTACHMENT E

CAUSE NO. 24-08-12392

| | | |
|--------------------------------|---|---|
| STATE OF TEXAS, |) | |
| <i>Plaintiff,</i> |) | |
| |) | |
| v. |) | IN THE DISTRICT COURT OF |
| |) | |
| GENERAL MOTORS LLC, and |) | MONTGOMERY COUNTY, |
| ONSTAR LLC, |) | TEXAS |
| |) | Montgomery County - 457th Judicial District Court |
| |) | |
| |) | _____ JUDICIAL DISTRICT |
| |) | |
| <i>Defendants.</i> |) | JURY TRIAL DEMANDED |
| _____ |) | |

PLAINTIFF'S ORIGINAL PETITION

Plaintiff, STATE OF TEXAS (the “Plaintiff” or “State”), acting by and through the Attorney General of Texas, Ken Paxton, brings this action against Defendants GENERAL MOTORS LLC (“General Motors” or “GM”) and ONSTAR LLC (“OnStar”) for violating the Texas Deceptive Trade Practices—Consumer Protection Act (“DTPA”), Tex. Bus. & Com. Code §§ 17.41–17.63.

INTRODUCTION

“At General Motors, your privacy is important to us, as is your trust in our products or services.” – General Motors’ Privacy Statement (July 1, 2023)

1. When consumers purchase a vehicle, their primary concern is how effectively it will get them from Point A to Point B. But for years, consumers who purchased GM vehicles also unwittingly opted into an all-seeing surveillance system. General Motors deceptively collected scores of data points from consumers about their driving habits, monetized that data by selling it to other commercial actors, and permitted those actors to use the ill-gotten data to make adverse decisions when dealing with those same consumers. Customers of General Motors thought that when they purchased a vehicle, they were merely acquiring a mode of transportation. But in fact, these consumers were making a decision that would follow them and have consequences in multiple unrelated transactions with unrelated vendors for years to come.

2. Since 2015, General Motors has installed technology in its vehicles that it advertised as improving the safety, functionality, and operability of its vehicles. But this technology can also collect, record, analyze, and transmit highly specific “Driving Data” about a vehicle’s usage. And for years, Defendants General Motors and its subsidiary, OnStar LLC (collectively, “General Motors” or “GM”), have unlawfully collected, used, and sold the Driving Data it obtained through this technology.

3. The Driving Data collected and sold by General Motors included data from over 14 million of its vehicles, and the data of more than 1.8 million Texans. That Driving Data consisted of the date, start time, end time, vehicle speed, driver and passenger seatbelt status, and distance driven each time a customer drove their GM vehicle. The Driving Data also consisted of information about customers’ use of other GM products, including data collected from General Motors’ mobile apps.

4. Moreover, General Motors' unlawful sale of Driving Data was a systemic part of its operations, formalized through agreements with various companies. For example, GM entered into agreements requiring purchasing companies to build a database called a "telematics exchange" to house the purchased Driving Data. Under these agreements, the purchasing companies were to use the Driving Data to calculate a customer "Driving Score" based on risk "factors" developed by General Motors. Purportedly "bad" driving factors included late-night driving, driver and passenger seat belt status, instances of sharp turns, and hard braking, hard acceleration events, and driving over 80 miles per hour.

5. GM's agreements required these same purchasing companies to license access to their respective telematics exchanges to car insurance companies ("Insurers"). After buying a license, an Insurer could access the respective Driving Scores of the more than 16 million customers whose data General Motors sold. Unbeknownst to these customers, Insurers could—and did—use these scores and data to make significant decisions that impacted customers including monthly premium increases, dropped coverage, or coverage denials.

6. General Motors profited handsomely from these agreements. The sale of Driving Data generated multiple new revenue streams for GM. It unlocked millions in lump sum payments, "royalty payments" based on telematics exchange licenses sold to Insurers, and annual guaranteed payments if GM sold the Driving Data of a threshold number of newly sold vehicles.

7. General Motors represented to purchasing companies that its customers had consented to the collection, use, and sale of their Driving Data. However, as detailed in the "Factual Allegations" below, General Motors engaged in a series of misleading and deceptive acts and practices to obtain these customers' "consent" to enroll in OnStar products, including Connected

Vehicle Services, General Motors' mobile apps (myChevrolet, myGMC, myBuick, and myCadillac), and the OnStar Guardian App.

8. GM's practice was to subject consumers who had just completed the time-consuming and stressful process of buying or leasing a vehicle at a dealership to an "onboarding" process. To customers, the onboarding process appeared to be a mandatory pre-requisite to taking ownership of their vehicle; however, it was no more than a deceptively designed sales flow to ensure that customers would sign up for GM's products and unwittingly be enrolled in GM's Driving Data collection scheme. As part of this onboarding process, General Motors electronically presented customers with over fifty pages of disclosures about its OnStar products, which consisted of product descriptions and a confusing series of applicable user terms and privacy notices.

9. GM purported to disclose its privacy practices to consumers, but its disclosures were confusing and highly misleading. The disclosures touted the "customer benefits" of GM's products, and falsely implied that data collected by General Motors would be used for reasons related primarily to improve the safety, functionality, and operability of its vehicles and products by GM and its partners. For example, in one disclosure, General Motors stated that it "may use [customers'] information to develop, enhance, provide, service, maintain, and improve the safety, security, and quality of [its] products, programs, and services, and for product research and marketing[.]" Similarly, another disclosure stated that General Motors would share customers' information with other companies for only certain reasons, such as "to develop, enhance, provide, service, maintain, and improve the safety, security, and quality of [its] products, programs, and services, to respond to [customers'] requests, to allow recipients to use it for marketing, and as required or permitted by law."

10. In actuality, General Motors used its lengthy and detailed disclosures to obfuscate its deceptive and harmful conduct. At no point did General Motors inform customers that its practice was to sell *any* of their data, much less their *Driving Data*; nor did General Motors disclose that it had contracts in place to make its customers' Driving Scores available to other companies; nor did General Motors disclose that it contracted to permit companies to re-sell customers' Driving Scores to Insurers.

11. Moreover, as detailed in the factual allegations below, General Motors incentivized dealership employees, often through commissions, to enroll customers in its Driving Data collection scheme which, on information and belief, resulted in many customers being enrolled without their knowledge or consent. Further, if a customer attempted to decline to enroll, they would be shown various "warning" messages which represented that declining would result in the de-activation of several of their vehicle's safety features.

12. The State of Texas contends that this proceeding is in the public interest and brings this action to end the complained-of harmful and unlawful practices and penalize General Motors for its false, deceptive, and misleading conduct.

JURISDICTION AND VENUE

13. This action is brought by the Texas Attorney General's Office through its Consumer Protection Division in the name of the State of Texas ("Plaintiff" or the "State") and in the public interest, pursuant to the authority granted by Section 17.47 of the Texas Deceptive Trade Practices Act ("DTPA"). The State brings this action on the grounds that General Motors has engaged in "false, deceptive, and misleading acts and practices in the course of trade and commerce" as defined in, and declared unlawful by, Subsections 17.46(a) and (b) of the DTPA, at all times described below.

14. In enforcement actions filed pursuant to Section 17.47 of the DTPA, the Attorney General may seek civil penalties, redress for consumers, and injunctive relief. In addition, the Attorney General may pursue reasonable attorney's fees and litigation expenses in connection with the prosecution of the instant action, in accord with Texas Government Code section 402.006(c).

15. Venue of this suit lies in Montgomery County, Texas, pursuant to Section 17.47(b) of the DTPA because Defendants have done business in Montgomery County and because transactions at issue in this suit have occurred in Montgomery County.

DISCOVERY

16. The discovery in this case should be conducted under Level 3 pursuant to Texas Rule of Civil Procedure 190.4. Restrictions concerning expedited discovery under Texas Rule of Civil Procedure 169 do not apply because the State seeks non-monetary injunctive relief as part of its claims.

17. In addition to injunctive relief, the State claims entitlement to monetary relief in an amount greater than \$1,000,000.00, including civil penalties, reasonable attorney's fees, litigation expenses, restitution, and costs.

DEFENDANTS

18. **Defendant General Motors LLC** ("General Motors" or "GM") is a United States public corporation headquartered in Detroit, Michigan, and incorporated under the laws of Delaware. General Motors is a multinational automotive manufacturer known for owning and manufacturing four automobile brands: Chevrolet, GMC, Cadillac, and Buick. At the time of filing, Defendant's agent for service of process in Texas is the Corporation Services Company, 217 East 7th Street, Austin, TX 78701-4234.

19. **Defendant OnStar LLC** ("OnStar") is a United States corporation headquartered in Detroit, Michigan, and incorporated under the laws of Delaware. OnStar is a subsidiary of

General Motors that provides subscription-based communications, in-vehicle security, emergency services, turn-by-turn navigation, and remote diagnostics systems throughout the United States. At the time of filing, Defendant's agent for service of process in Texas is the Corporation Services Company, 217 East 7th Street, Austin, TX 78701-4234.

TRADE AND COMMERCE

20. At all times described below, Defendants and their agents have engaged in conduct that constitutes "trade" and "commerce" as defined in Section 17.45(6) of the DTPA.

PUBLIC INTEREST

21. The State has reason to believe that General Motors is engaging in or has engaged in the unlawful acts or practices set forth below. In addition, the State has reason to believe that General Motors has caused injury, loss, and damage to the State, and has caused adverse effects to the lawful conduct of trade and commerce, thereby directly or indirectly affecting the people of this State. Therefore, the Consumer Protection Division of the Office of the Attorney General initiates this proceeding in the public interest. *See* DTPA § 17.47.

PRE-SUIT NOTICE

22. The Consumer Protection Division provided General Motors notice of the general nature of unlawful conduct challenged herein at least seven days before filing suit, as may be required by Section 17.47(a) of the DTPA.

FACTS

23. General Motors is one of the largest multinational automotive manufacturing companies in the world. Since 2015, General Motors has sold or leased over 1.5 million vehicles under its four brands (Chevrolet, GMC, Cadillac, and Buick) to customers in the State of Texas. In 2023 alone, General Motors manufactured and delivered over 275,000 vehicles across its four

brands to Texas consumers, operated eighteen facilities in the State of Texas, and maintained a network of over 300 dealerships in the State of Texas, including in Montgomery County. GM's agreements with dealerships authorized those dealerships to advertise, offer, and sell GM's products and services, including its subscription-based products, in accordance with General Motors' requirements and specifications.

24. Beginning in 2005, General Motors began partnering with car insurance carriers ("Insurers") to provide usage-based insurance plans to its customers. Under these original, usage-based plans, customers could receive a discount from their Insurer if they exhibited "good" driving behavior. To show "good" driving behavior, customers would install an Insurer-provided device into their vehicle that monitored their Driving Data.

25. As technology advanced, however, Insurer-provided devices were no longer necessary. Rather, General Motors began manufacturing vehicles equipped with technology known as telematics systems. Using a vehicle's telematics system, General Motors was able to directly obtain the same data from its vehicles that the Insurer-provided devices would have otherwise collected.

26. The telematics system is composed of both hardware and software. The hardware component consists of internal and external cameras, a range of sensors (such as seat and seatbelt sensors), speakers, and microphones. The software component is produced by OnStar and has been installed in almost all vehicles manufactured by General Motors since 2015.

27. General Motors captured Texans' data using GM vehicles' telematics systems, and the mobile apps GM provided to customers. Unlike the original usage-based insurance programs that require customers to install an optional device, and which use Driving Data to reward "good" driving behavior, General Motors used the telematics system to unilaterally collect its customers'

Driving Data, analyze it, and sell it in a manner that, unbeknownst to its customers, *penalized* their “bad” driving behavior.

28. General Motors’ telematics system collects an enormous amount of Driving Data.

Those types of Driving Data collected and sold include:

- (a) synthetic key;
- (b) trip ID;
- (c) element timestamp;
- (d) event code;
- (e) element code;
- (f) element value;
- (g) obsolete GPS data indicator;
- (h) current speed;
- (i) current speed validity indicator;
- (j) GPS direction;
- (k) driver seat belt status;
- (l) GPS estimated horizontal positioning error;
- (m) GPS elevation;
- (n) engine idle run time total supported indicator;
- (o) engine idle run time total;
- (p) engine PTO active run time total;
- (q) engine run total supported indicator;
- (r) engine PTO active total run time supported indicator;
- (s) engine run time total;

- (t) total fuel used;
- (u) GPS time;
- (v) GPS latitude coordinate;
- (w) lifetime energy used;
- (x) GPS longitude coordinate;
- (y) location time offset;
- (z) odometer reading;
- (aa) speed rate of change;
- (bb) speed rate of change positive indicator;
- (cc) vehicle ignition system power mode;
- (dd) driver seatbelt latched;
- (ee) hard acceleration occurs;
- (ff) hard brake occurs;
- (gg) ignition off;
- (hh) ignition on;
- (ii) speed over 80 miles per hour; and
- (jj) speed under 80 miles per hour.

I. General Motors aggressively touted the benefits of its products while obfuscating its privacy practices so it could collect and sell customers' Driving Data.

29. General Motors aggressively strived to enroll customers that purchased a 2015 model year or newer GM vehicle into signing up for GM products including (1) "Connected Vehicle Services," which GM uses as a catch-all term to describe the features it can enable using a vehicle's telematics system; (2) General Motors' mobile apps; and (3) the OnStar Guardian App.

30. The specific features of these products varied but they all had one key feature in common: signing up resulted in customers' unwittingly agreeing to GM's using these products to collect and sell their Driving Data to other companies—including Insurers. Each product is discussed in turn.

a. General Motors aggressively marketed the benefits of its Connected Vehicle Services.

31. General Motors marketed the Connected Vehicle Services as giving customers “better drives,” “better entertainment,” “better safety,” and “better control.” General Motors offered customers the Connected Vehicle Services through several different subscription plans. The subscription plans GM offered have changed over time, but as of 2018 were: (1) Connected Access for no charge; (2) Remote Access for \$14.99 per month; (3) Unlimited Access for \$39.99 per month; (4) Safety & Security for \$24.99 per month; (5) Remote Access + Safety & Security for \$34.99 per month; and (6) Unlimited Access + Safety & Security for \$59.99 per month.

32. The free Connected Access plan included five features (all of which were included with each of the paid subscription plans). The five basic features as described by General Motors were:

- (a) OnStar Smart Driver (“Smart Driver”): “provide[s] [a customer] with insights on [their] driving behavior and can help [them] recognize driving improvement opportunities” and “provides this feedback in the form of an easy-to-read monthly report and a Smart Driver score.”
- (b) OnStar Vehicle Diagnostics (“OVD”): provides customers with “easy-to-use monthly diagnostics reports showing the health of [their] vehicle’s key operating systems.”

- (c) OnStar Dealer Maintenance Notifications: sends a customer's dealership their "vehicle diagnostics reports so [their dealer] can contact [them] to set up a service appointment, if needed."
- (d) OnStar Marketplace: provides customers with "valuable offers on the go to the places [a customer] like[s] to eat, shop and play."
- (e) OnStar In-Vehicle Apps: lets customers "[m]ake the most of [their] drive time by streaming [their] favorite music, sports and entertainment."

b. General Motors also pushed customers to download its free mobile apps, which it then used to collect and sell their Driving Data.

33. General Motors also strived to get as many customers as possible to download one of its brand-specific mobile apps: myChevrolet, myGMC, myBuick, or myCadillac. GM made these apps available at no cost but unbeknownst to customers, GM treated the downloading and enrolling of the app as the customer's "agreement" to the collection and sale of their Driving Data.

34. General Motors advertised the apps as a "mobile command center for your vehicle" that would provide customers with a "user-friendly way to leverage many of the basic and available connectivity and vehicle management features offered through [OnStar]." The mobile apps' features included the ability to track a vehicle's location, check its odometer reading, fuel level, and oil life, lock and unlock its doors, and remotely turn the vehicle on or off.

c. General Motors enticed customers to sign up for OnStar Guardian by highlighting its extra safety features, and then used it to collect and sell more information about its customers.

35. General Motors touted the safety benefits of the OnStar Guardian App to entice customers into signing up. Unbeknownst to customers, however, GM treated a customer's enrollment in this product of the app as the customer's "agreement" to the collection and sale of their Driving Data.

36. General Motors advertised OnStar Guardian as providing “family safety that goes where you go.” By enrolling in this product, customers could access many of the safety features provided through the Connected Vehicle Services even if they were not in or operating their vehicle.

OnStar Services Wherever You Are With the OnStar Guardian app

Thanks to OnStar, you may feel safer in your car. But how about when you or your family are in someone else’s car? Or on your motorcycle? Or at home? Or out for a walk or hike? We’ve got you. The OnStar Guardian® app* gives your family the key safety services of OnStar — Roadside Assistance,* GPS locator service,* emergency help — even crash detection — anywhere you go. You can share the app with up to seven friends or family members.*

Figure 1. General Motors touted the safety features of OnStar Guardian to encourage customers to enroll.

37. The Guardian App also included several additional features, such as the ability to access the sensors in a customer’s phone to monitor if they were in a car crash and the ability to track a person’s location using their phone. Customers could also “share” the OnStar Guardian App with up to seven other people who could then access its features as well.

38. On information and belief, General Motors was able to use the OnStar Guardian App to collect and sell additional data about its customers and anyone with whom their customers shared the OnStar Guardian App.

II. General Motors used several deceptive techniques to ensure customers would enroll in its Connected Vehicle Services.

39. General Motors pushed customers into enrolling in its Connected Vehicle Services through a series of deceptive and misleading practices, including through its aggressive “onboarding” process, all of which impaired customers’ decision making and ensured they would enroll in the Connected Vehicle Services.

a. General Motors used dealership employees to pressure customers into enrolling in the Connected Vehicle Services using GM's onboarding process.

40. General Motors incentivized dealership employees, often through commissions, to use GM's onboarding process to enroll customers in the Connected Vehicle Services before they left the dealership. On information and belief, this commission-based model resulted in many customers being enrolled in the Connected Vehicle Services without their knowledge or consent.

41. For customers that *were* taken through GM's onboarding process, the onboarding process appeared to be a mandatory pre-requisite to taking ownership of their vehicle. However, the onboarding process was no more than a deceptively designed sales flow to ensure that customers would sign up for the Connected Vehicle Services and unwittingly be enrolled in GM's Driving Data collection scheme.

42. To conduct the onboarding process, a dealership employee would log into GM's onboarding system, enter the customer's VIN number, create an OnStar account for the customer or locate the customer's pre-existing account, and then GM's system would list the Connected Vehicle Services subscription plans that the vehicle was eligible for (including the free Connected Access plan).

43. At this point, GM's system instructed the employee to show the screen to the customer, which displayed a message that further made the onboarding process appear mandatory. Specifically, the screen instructed the customer to "complete the next few steps" "before tak[ing] ownership of [their] vehicle," and prompted the customer to select a "Get started" button. On information and belief, neither GM nor dealership employees informed customers that they were not required to complete the onboarding process.

b. General Motors did not give customers a meaningful opportunity to review its deceptive disclosures.

44. After selecting the “Get started” button, General Motors overwhelmed customers with information by providing them a screen containing a 29-page “User Terms for Connected Vehicle Services,” an 18-page “General Motors U.S. Connected Services Privacy Statement,” a link to AT&T’s terms and conditions, a link to AT&T’s network management practices, a vehicle ownership acknowledgment statement, and, finally, an “I accept” and an “I decline” checkbox option, with both options including even more information.

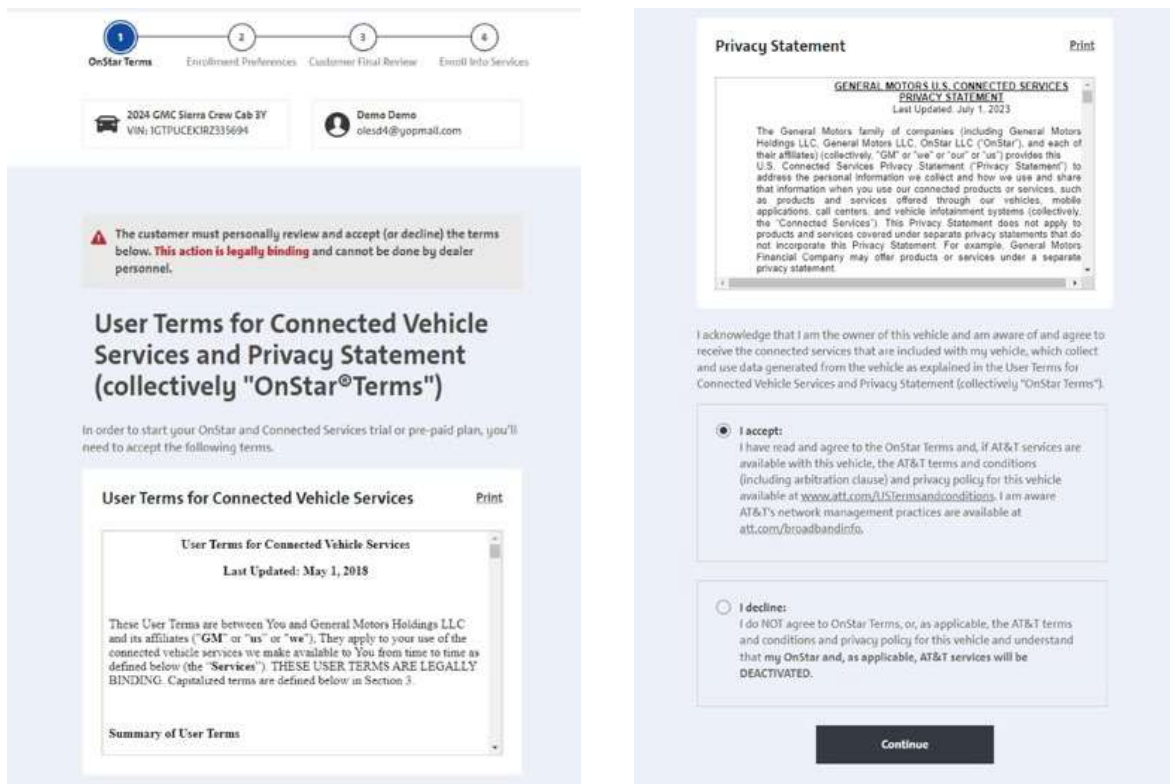


Figure 2. Customers were only shown the first paragraph of the two policies and needed to scroll to review them. But as explained, neither of these policies disclosed the actual nature of GM’s conduct.

45. The substantial information on this screen served to prevent and deter customers from reviewing GM’s disclosures. Moreover, as explained *supra*, even if a customer closely reviewed every word on this screen, the disclosures, and the other linked policies, they still would

have no knowledge of GM’s actual conduct. Specifically, nowhere did the disclosures explain that by selecting the “I accept” option, customers were activating the five basic OnStar features: Smart Driver, Vehicle Diagnostics, Dealer Maintenance Notifications, Marketplace, and In-Vehicle Apps. Nor did these disclosures explain that by activating those features, customers were “agreeing” to GM’s collection and sale of their Driving Data.

c. General Motors presented customers with safety “warning” messages if they tried to decline the Connected Vehicle Services.

46. General Motors also designed the onboarding process to repeatedly display messages meant to deter customers from declining the Connected Vehicle Services. Specifically, any customer that selected the “I decline” option received a “warning” message that misleadingly claimed that declining would result in the deactivation of the Connected Vehicle Services, even though at this point in the onboarding process customers had not yet enrolled in the Connected Vehicle Services.

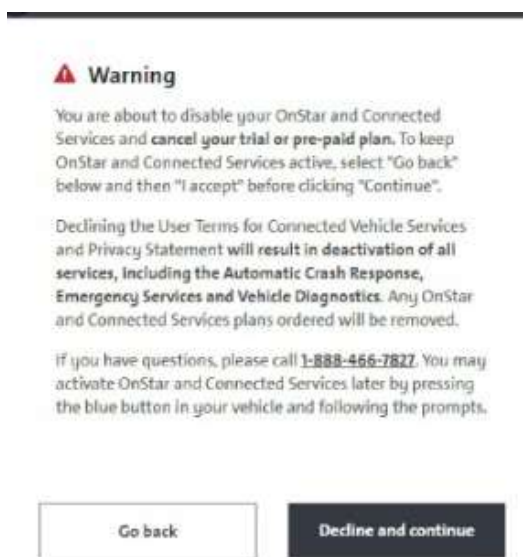


Figure 3. The “warning” message deterred customers from canceling by emphasizing in bold letters that by declining, the customer was deactivating their vehicle’s safety features.

47. The warning message further attempted to dissuade customers from declining the Connected Vehicle Services by emphasizing that safety features, such as “Automatic Crash Response” and “Emergency Services,” would be de-activated if they declined.

48. If GM’s first safety warning did not successfully deter a customer, the customer would be presented with another screen attempting to dissuade them from declining the Connected Vehicle Services. Specifically, GM displayed a message explaining the “consequences” of declining the Connected Vehicle Services and prompted the customer to “go back and accept OnStar terms.”

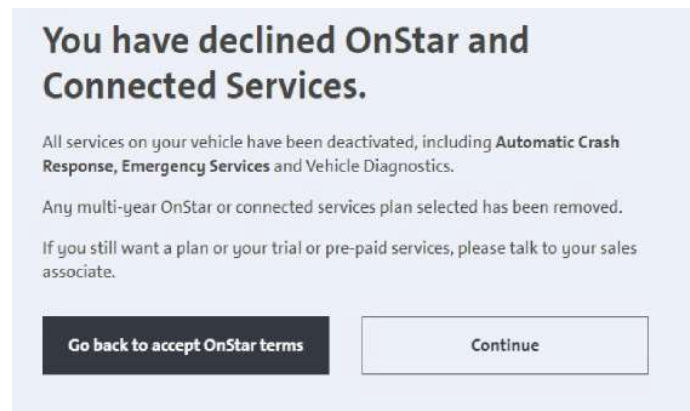


Figure 4. After rejecting the services twice, GM again tried to get customers to reverse their decision.

49. If a customer managed to leave the dealership without enrolling in the Connected Vehicle Services, General Motors would repeatedly email them to sign up for a “trial” period of the Connected Vehicle Services.

50. While General Motors aggressively enrolled as many customers as possible, it simultaneously made it difficult for customers to cancel their Connected Vehicle Services plan. Specifically, while General Motors permitted customers to enroll in the Connected Vehicle Services using a variety of methods, including online, on information and belief, GM only allowed customers to cancel the Connected Vehicle Services by calling.

51. For GM’s mobile apps, like the Connected Vehicle Services, General Motors prompted customers to download its app before they left the dealership as part of GM’s “onboarding” process. If a customer did not download the app at the dealership, on information

and belief, General Motors would repeatedly email customers “reminding” them to download the app.

III. GM’s user terms and privacy notices misled and confused customers about GM’s collection, use, and sale of their Driving Data.

52. General Motors maintained and provided customers with lengthy and detailed disclosures about its products, and provided them to customers during its dealership onboarding process and on its websites and apps. GM’s disclosures generally consisted of “user terms” and “privacy statements,” and as of July 1, 2023, included a 29-page “User Terms for Connected Vehicle Services,” an 18-page “U.S. Connected Services Privacy Statement,” a link to a 46-page AT&T “Consumer Service Agreement,” a link to AT&T’s “Broadband Information” website, and if a customer downloaded the mobile app when prompted or enrolled in OnStar Guardian, an additional 3-page “User Terms for Application Services,” a 6-page “Account Guidelines,” and a 4-page “Privacy Statement for Application Services,” and a 3-page “OnStar Guardian Privacy Statement.” While GM’s disclosures have varied over time, at no point have they materially disclosed anything above and beyond that described below.

53. GM’s various user terms for its products generally included lengthy and dense explanations of the obligations, legal rights, and remedies applicable to GM and its customers, as well as cross-references to GM’s various privacy statements and other applicable user terms. GM’s multiple privacy statements generally included summaries that purported to highlight the “key points” of GM’s collection, use, and “sharing” of customers’ information, and were followed by lengthy explanations of nearly every aspect of GM’s information practices, including a verbose yet vague explanation of GM’s collection, use, and sharing of customers’ data, as well as cross-references to GM’s various user terms and other applicable privacy statements.

54. While the specifics of GM’s various user terms and privacy statements varied, they all shared several things in common—none of them informed customers that GM would *sell* any of their data; nor did they disclose that GM would sell their Driving Data; nor did they disclose that GM would use their Driving Data to profit and receive royalty payments; nor did they disclose that GM contractually required companies to create databases of their Driving Data; nor did they disclose that GM would use the Driving Data to create risk profiles of its customers (i.e., Driving Scores); nor did they disclose that GM would make customers’ Driving Scores available to other companies; nor did they disclose that GM expressly permitted companies to re-sell their Driving Scores to Insurers; nor did they disclose that agreeing to use GM’s products could result in financial harm.

55. Further, GM left customers with the impression that it did not sell their data, and specifically failed to disclose that it was actively engaged in using their Driving Data to generate Driving Scores or that it was selling their Driving Score and Driving Data to several companies, including Insurers whose use of the Driving Data could result in financial harm to customers.

56. GM’s multiple agreements to sell customers’ data since 2015, as detailed *supra*, underscore the false, misleading, and deceptive nature of GM’s conduct.

a. GM’s U.S. Connected Services Privacy Statement contained false and misleading representations and caused confusion regarding GM’s collection, use, and sale of Driving Data.

57. To ensure that customers enrolled in its Driving Data collection scheme, GM’s disclosures misleadingly focused on the “customer benefits” of its products and that its products would give customers “better drives,” “better entertainment,” “better safety,” and “better control.”

58. To further ensure that customers would enroll in its products, GM made a series of misleading statements that the data it collected would be used to improve the safety, functionality, and operability of its vehicles. For example, in the “key points” of its “U.S. Connected Services

Privacy Statement,” General Motors represented that it “may use [customers’] information to develop, enhance, provide, service, maintain, and improve the safety, security, and quality of [its] products, programs, and services, and for product research and marketing[.]”

59. In its next key point, General Motors stated that it would share customers’ information with other companies primarily “to develop, enhance, provide, service, maintain, and improve the safety, security, and quality of [its] products, programs, and services, to respond to [customers’] requests, to allow recipients to use it for marketing, and as required or permitted by law.” With respect to retaining customers’ information, GM also highlighted that it would keep customers’ information only “for as long as necessary to provide products or services to [customers]. . . .”

60. Another section of GM’s U.S. Connected Privacy Statement, titled “How we may share your information,” purports to disclose how GM would share customers’ information. In this section, GM included the universe of the types of parties with whom it may share customers’ information, and included a “Third-Party Business Relationships” subsection that contained a specific example of when it would share *any* information with an Insurer. GM’s example was buried at the end of a parenthetical at the end of a sentence and obliquely indicated that “*usage based insurance providers*” “may” be given GM data, but only if the consumer had “receive[d] a service from them and/or authorized them to request data from GM.” (italics in original).

HOW WE MAY SHARE YOUR INFORMATION

We may share the categories of your information described above as follows:

GM Family of Companies: Within the GM family of companies (*for example, including OnStar*) for the above uses.

Emergency Service Providers: With emergency service providers, such as law enforcement, roadside assistance providers, and ambulance providers, to protect your safety or the safety of others, and to deliver related services (*for example, Stolen Vehicle Assistance Services*).

Third-Party Business Relationships: With business that GM enters into business relationships, such as SiriusXM, in connection with their products and services; research institutes, for research and development purposes (*for example, improving highway safety*); or dealers, fleet, or rental car companies, for service or maintenance of your vehicle. We may also share data with third parties for marketing activities (with necessary consents) or where you have elected to receive a service from them and/or authorized them to request data from GM (*for example, financial organizations who offer financing for the purchase or lease of GM vehicles or usage based insurance providers*).

Service Providers: With our product and service providers who work on our behalf in connection with the uses described in the preceding section, such as dealer managed service providers, wireless service providers (e.g. AT&T), companies that administer our contests and promotions, host and/or operate our websites, send communications, perform data analytics, process, store, or manage credit card, information (we will not otherwise share your credit card information).

Where Required or Permitted by Law: As required or permitted by law, such as in conjunction with a subpoena, government inquiry, litigation, dispute resolution, or similar legal process, when we believe in good faith that disclosure is necessary to protect our rights, your safety, or the safety of others, to detect, investigate and prevent fraud or other illegal activity, or to conduct screening to ensure you are not on any government list of restricted parties.

Business Transfers: With a prospective or completed sale, transfer, or financing of a part of a GM business or its assets.

Figure 5. “Usage based insurance” refers to insurance products offered by Insurers, such as those offered by General Motors’ subsidiary, GM Insurance, that require insureds to install an Insurer-provided device into their vehicle to be eligible for discounts based on “good” driving behavior.

61. While this is the only instance where GM even gestures toward the possibility of sharing *any* information with Insurers – and implies that it is shared only with a consumer’s authorization, it lumps this minimal disclosure in with utterly inapposite and unrelated information, such as that GM has business relationships with “SiriusXM” (a satellite radio company) and that it interacts with “research institutes” to “improv[e] highway safety” (italics omitted), to the point that the disclosure itself is meaningless.

62. The disclosure also contained confusing compound language, such as the notification—combined into a single sentence—that information may be shared “for marketing activities,” “where you have elected to receive a service” from someone, and if you “authorized” someone to receive the data. This compound language fails to give an ordinary consumer reasonable notice about whether all, some, or even any of these conditions are prerequisites to GM’s sharing of the customer’s information with third parties.

63. The only other instance in which GM mentioned “insurance” was in its 29-page User Terms for Connected Vehicle Services to clarify the unremarkable point that General Motors is not an insurance company.

b. GM’s privacy statements for its mobile apps and OnStar Guardian also contained false and misleading representations and caused confusion regarding GM’s collection, use, and sale of Driving Data.

64. GM’s Privacy Statement for Application Services and its OnStar Guardian Privacy Statement failed to disclose that GM was actively engaged in using customers’ data to create Driving Scores and selling those scores and the underlying Driving Data to Insurers, whose use of the data could result in financial harm to its customers.

65. GM’s Privacy Statement for Application Services purports to describe how GM and its affiliates “collect, use, and share information . . . when [a customer] download[s] this application to [their] phone or other Internet-connected device . . . and when [a customer] use[s] the services available through the Application.” Unlike the U.S. Connected Services Privacy Statement, however, the Privacy Statement for Application Services made no mention of “insurance” in its “Sharing of Information” section.

Sharing of Information

We may share information we collect about you as described in the OnStar Privacy Statement. For example, we share information with necessary third parties when you use the Application to make requests for third party or related services available through the Application, such as for dealer maintenance appointments or roadside assistance. We may share the location of your Device in the same manner as we share location and speed of your Vehicle. For example, we may share the location of your Device with:

- third party service providers working on our behalf,
- emergency service providers,
- others when required by law, and
- those you ask us to share this information with.

We may also share the location of your Device when necessary to provide the Application Services to you; to comply with legal obligations; to protect the safety and rights of you and others; for product safety and security purposes; and for the purposes described in the OnStar Privacy Statement.

Figure 6. General Motors listed the types of companies with whom it shared customers’ mobile app information, but made no mention of insurance.

66. The OnStar Guardian Privacy Statement contained a similar “Sharing of Information” section as that in the Privacy Statement for Application Services, and likewise omitted any mention of “insurance.”

Sharing of Information

We share your information as described in the OnStar Privacy Statement. For example, we share information with necessary third parties when you use the Application to make requests for third party or related services available through the Application, such as roadside assistance. We may share your information with:

- third party service providers working on our behalf;
- members and invitees of your “My Family”;
- emergency service providers;
- individuals specified by you when using the Application, such as emergency contacts;
- others when required or permitted by law, and
- those you ask us to share this information with.

We may share the location of your Device when necessary to provide the Application Services to you; to comply with legal obligations; to protect the safety and rights of you and others; for product safety and security purposes; and for the purposes described in the OnStar Privacy Statement.

Figure 7. General Motors listed the types of companies with whom it shared customers’ OnStar Guardian information, but made no mention of insurance.

67. GM’s Privacy Statement for Application Services and the OnStar Guardian Privacy Statement cause further confusion, because each informs consumers that they must also refer to the “OnStar Privacy Statement” because “together [they describe] our privacy practices.” On information and belief, there is no privacy statement titled “OnStar Privacy Statement,” and GM instead maintains a page called “OnStar Privacy Statement” which lists a series of privacy statements.

c. General Motors used Smart Driver to mislead customers about its harmful use and sale of their Driving Data.

68. General Motors also used its descriptions and disclosures associated with the OnStar “Smart Driver” feature to further confuse and mislead consumers, particularly regarding whether their Driving Data would be sold to other companies, provided to Insurers, or used to evaluate their insurance rate based on their Driving Score.

69. As noted *supra*, GM markets Smart Driver to customers as a tool for them to monitor their own driving behavior. Instead of disclosing any of the consequences of a “bad”

Driving Score, General Motors framed Smart Driver—and the score it generated—as a feature that was purely beneficial to customers. According to General Motors, Smart Driver “provides driving feedback that can help[sic] drivers improve their vehicle’s performance, drive more carefully, save on gas and help reduce wear and tear on the vehicle.” General Motors likewise de-emphasized the significance of a bad Driving Score:

What does your score tell you?

In summary, if you have a score of 88, yes, you might consider yourself a B+ driver — well above average. Unlike a permanent high school grade, though, your Smart Driver score isn’t permanent. With the regular feedback and tips for improving your score, you can make your Smart Driver score grow over time. Check how you compare (anonymously) with other Smart Drivers in your monthly report — you could find yourself among the highest-scoring Smart Drivers.

Figure 8. Instead of informing customers of the consequences of failing to improve their Driving Score, General Motors reassured them that their Driving Score was not permanent and could improve over time.

70. According to General Motors, it would “use information [it] collect[ed] about where and how [customers] operate [their] vehicles, such as [a] vehicle’s location, routes driven, driving schedule, fuel or charging levels, fuel economy, battery status, overall vehicle health, and driving behavior, such as hard braking, hard acceleration, tailgating, vehicle speed, late night driving, driver and passenger seatbelt status, and driver attention” to provide customers with insights about their driving behavior.

OnStar Smart Driver†

Improve your ownership experience with access to OnStar Smart Driver.

What is OnStar Smart Driver? OnStar Smart Driver provides you insights on your driving behavior and can help you recognize driving improvement opportunities. You'll earn achievements, get valuable feedback with each trip, and access your driving data. OnStar Smart Driver also gives you the opportunity to use Connected Teen Driver, which helps promote safe driving habits.

We'll use information we collect about where and how you operate your vehicle, such as your vehicle's location, routes driven, driving schedule, fuel or charging levels, fuel economy, battery status, overall vehicle health, and driving behavior, such as hard braking, hard acceleration, tailgating, vehicle speed, late night driving, driver and passenger seatbelt status, and driver attention. Smart Driver "hard braking" and "hard acceleration" events are identified when measured vehicle speed changes rapidly, regardless of the cause of the rapid speed change. We may also use alerts from your vehicle, such as forward collision and traction control.

After enrollment, you can opt out of OnStar Smart Driver at any time by clicking "unenroll" in OnStar Smart Driver in your myGMC mobile app.

Figure 9. Before leaving the dealership, customers were shown this description touting the benefits of Smart Driver and encouraging them to enroll.

IV. For nearly a decade, General Motors compiled and sold customers' Driving Data collected as part of providing its products without their knowledge.

71. In 2015, General Motors entered into the first of many agreements to sell its customers' Driving Data. Over the course of nearly a decade, General Motors continued to sell, re-sell, and have other companies license out access to its customers' Driving Data, oftentimes in a manner it knew would financially harm those customers. On information and belief, General Motors sold over 16 million of its customers' Driving Data to other companies, including the data of 1.8 million Texans.

72. Taking its harmful conduct further, General Motors contractually obligated at least one of the purchasing companies to attempt to purchase the Driving Data of other car manufacturers' customers. In return, General Motors would receive additional profit from the sale of Driving Data from these other car manufacturers. General Motors' mandate was successful, as set forth in greater detail below.

a. GM's 2015 Agreement with Verisk Analytics Inc.

73. General Motors first entered into an agreement with Verisk Analytics Inc. (“Verisk”) to sell its customers’ Driving Data on October 22, 2015 (“Verisk Agreement”). Verisk is a data analytics and risk assessment firm focused on providing insurance companies with “innovative solutions to meet customer needs and drive growth.”

74. Pursuant to the Verisk Agreement, General Motors received an initial multi-million-dollar lump sum payment from Verisk. Going forward, General Motors periodically sent Verisk the additional Driving Data it collected from its customers. Further, General Motors represented to Verisk that it received its customers’ consent to sell their Driving Data.

75. The Verisk Agreement also contractually required Verisk to develop a database, called a “Telematics Data Exchange” (hereinafter, “Verisk Exchange”), to house the Driving Data received from General Motors and use the Driving Data to calculate a “Driving Score” for each of GM’s customers.

76. A customer’s Driving Score was based on a series of “factors” developed by General Motors that were supposedly indicative of “bad” driving behavior and included behavior such as (1) unique identifiers of a trip; (2) trip mileage; (3) hard braking and acceleration events; (4) speed events over 80 miles per hour; and (5) other behavior tracked by OnStar Vehicle Diagnostics (“OVD”). Under the Verisk Agreement, GM provided Verisk with the Driving Data necessary to determine whether a customer exhibited any “bad” driving behaviors.

77. General Motors also sold its customers’ personally identifiable information to Verisk, including their customer ID, name, home address, OVD enrollment date, OVD unenrollment date, VIN, vehicle year, vehicle make, and vehicle model. In combination with the

Driving Data, this personally identifiable information allowed Verisk to create a Driving Score for each of GM's customers.

78. To further monetize the Driving Data, General Motors contractually required Verisk to market and sell licenses to Insurers to access the Verisk Exchange. Based on the revenue generated from Verisk's license sales to Insurers, Verisk paid General Motors ongoing "royalty payments."

79. Upon purchasing a Verisk Exchange license, Insurers could use the Verisk Exchange to search for the Driving Scores of their insureds or potential insureds and then use that information to financially harm General Motors' customers, including by denying prospective insureds coverage, increasing current insureds' monthly premiums, or dropping their current insureds from coverage entirely. Over the life of the Verisk Agreement, Verisk sold Verisk Exchange licenses to nine Insurers, and those Insurers accessed the Driving Scores of hundreds of thousands of GM's customers.

80. General Motors also contractually required Verisk to solicit "other vehicle [manufacturers], telecom carriers, and other third parties possessing Driving Data and other relevant vehicle data" for inclusion in the Verisk Exchange. Verisk succeeded and entered into similar agreements with both American Honda Motor Company on December 7, 2017, and Hyundai Motor America on March 1, 2018.

b. GM's 2018 Agreement with Wejo Limited

81. On December 21, 2018, General Motors entered into an agreement with Wejo Limited ("Wejo"), a British connected car start-up. Like the Verisk Agreement, General Motors sold Wejo the Driving Data so that Wejo could sell licenses for other companies to access the Driving Data. But unlike the Verisk Agreement, the Wejo Agreement authorized Wejo to pursue

potential buyers in other sectors, not just Insurers, and to sell the Driving Data only after receiving approval from GM.

82. Pursuant to the Wejo Agreement, General Motors bought a 35 percent ownership interest in Wejo for \$25 million and agreed to provide Wejo with the 2018 Driving Data of 2.6 million vehicles, valued at \$70 million. Going forward, General Motors continuously sent Wejo newly collected Driving Data. Like the Verisk Agreement, General Motors received ongoing payments from Wejo based on Wejo's license sales. Specifically, under the Wejo Agreement, Wejo had a minimum monthly revenue licensing target of \$3 million per month and Wejo agreed to pay General Motors 70 percent of this revenue. Wejo also agreed to "reimburse" GM if it ever failed to meet its monthly revenue target. This relationship continued until Wejo declared bankruptcy in May 2023.

83. The Driving Data General Motors sold to Wejo varied over time, but generally consisted of Driving Data underlying certain "Element Codes." These were based on factors similar to those developed by General Motors pursuant to the Verisk Agreement: (1) trip start; (2) trip end; (3) hard braking and acceleration events; (4) speed events over 80 miles per hour; and (5) driver seatbelt status change.

84. Over time, General Motors began selling additional types of Driving Data to Wejo. For example, in December 2022 General Motors started providing Wejo with its customers' "Radio Listening Data," which included data such as: (1) ignition state and timestamp (start or end of the trip); (2) AM/FM frequency data; (3) time zone identifiers; (4) radio station call sign; and (5) channel genre.

c. GM's 2019 Agreement with LexisNexis Risk Solutions

85. General Motors entered into a similar agreement with LexisNexis Risk Solutions (“LNRS”) on August 1, 2019 (“LNRS Agreement”), in which LNRS would “market and deliver FCRA and non-FCRA products and solutions to Insurers.”

86. Pursuant to the LNRS Agreement, LNRS paid General Motors an initial multi-million-dollar lump sum in exchange for the Driving Data that GM previously collected in 2017, 2018, and 2019. Going forward, General Motors periodically sent LNRS the additional Driving Data it collected from its customers.

87. General Motors also sought to profit off its ability to “potentially influence” other vehicle manufacturers to sell their respective Driving Data to LNRS. Specifically, LNRS agreed to pay GM additional royalty payments if LNRS successfully contracted with any “target OEMs,” which included American Honda Motor Co., Inc., Hyundai USA, Toyota Motor North America, and Volkswagen Group of America. On information and belief, none of the four “target OEMs” entered into agreements with LNRS (although as explained above, American Honda Motor Company and Hyundai Motor America entered into agreements with Verisk). However, LNRS entered into similar agreements with Mitsubishi Motors North America, Inc. on May 31, 2018, Nissan North America, Inc. on February 28, 2019,¹ Ford Motor Company on August 2, 2021, Subaru of America, Inc. on February 6, 2023, and Kia America, Inc. on October 16, 2023.

88. Like in the Verisk Agreement, the Driving Data sold by General Motors was housed in a database called the “LexisNexis Telematics Exchange” (“LNRS Exchange”), and the Driving Data was used to calculate a “Driving Score” for each of GM’s customers.

¹ This agreement expired in 2023 and, on information and belief, was never renewed.

89. A customer's Driving Score was also based on a series of "Driving Events" that were supposedly indicative of "bad" driving behavior. The Driving Events varied over time but included events such as: (1) ignition on, (2) ignition off, (3) hard brake occurrences, (4) hard acceleration occurrences, (5) time spent driving over 80 miles per hour, (6) time spent driving under 80 miles per hour, and (7) driver seatbelt status. Under the LNRS Agreement, GM provided LNRS with the Driving Data necessary to determine whether a Driving Event occurred in a customer's vehicle.

90. General Motors also sold LNRS its customers' personally identifiable information, including the customer's name, address, phone number, email address, and their vehicle's VIN, make, model, and year. In combination with the Driving Data, this personally identifiable information allowed LNRS to create a Driving Score for each of GM's customers.

91. Similar to the Verisk Agreement, General Motors contractually required LNRS to market and sell licenses to Insurers to access the LNRS Exchange. Based on the revenue generated from the license sales, LNRS paid General Motors ongoing "revenue share" payments.

92. For Insurers that contracted to use the LNRS Exchange, any time an individual made an inquiry about obtaining car insurance, the Insurer receiving the inquiry could search the LNRS Exchange to see if it contained Driving Data about the potential insured. In addition, LNRS agreed to annually pay General Motors a guaranteed minimum payment if GM provided LNRS with the Driving Data of a certain percentage of the vehicles it sold that year.

93. Like the Insurers that purchased licenses to use the Verisk Exchange, Insurers using the LNRS Exchange could search for information about their insureds and increase their insureds' monthly premiums or drop their insureds from coverage entirely.

d. GM's 2024 Agreement with Jacobs Engineering Group Inc.

94. On information and belief, General Motors most recently sold Driving Data to Jacobs Engineering Group Inc. ("Jacobs") on January 3, 2024. Jacobs is a professional services firm that provides engineering, technical, professional, and construction services. Pursuant to the agreement with Jacobs, General Motors authorized Jacobs to use de-identified Driving Data in Jacobs' own products and to license Driving Data to other parties approved by General Motors.

95. Like in the Verisk, LNRS, and Wejo Agreements, General Motors received revenue-sharing payments from Jacobs based on Jacobs' licensing of the Driving Data to third parties.

VIOLATIONS OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT

96. The State incorporates and adopts by reference the allegations contained in each and every preceding paragraph of this Petition, as if fully set forth herein.

97. The Texas Deceptive Trade Practices Act prohibits false, misleading, or deceptive acts or practices in the conduct of trade and commerce. As alleged herein and detailed above, Defendants have in the course and conduct of trade and commerce engaged in false, misleading, or deceptive acts or practices declared unlawful by and in violation of Section 17.46(a) and (b) of the DTPA.

Count I: Misrepresentations Regarding Its Products

98. Defendants falsely, expressly or by implication, misrepresented the benefits and risks of its products and their related features to consumers. While touting the benefits of its products as providing customers with "better drives," "better entertainment," "better safety," and "better control," Defendants were silent as to risks associated with their information sharing practices. Moreover, Defendants repeatedly sold their data in a manner it knew could financially

harm consumers through higher car insurance premiums, being dropped from coverage, or being denied coverage.

99. In doing so, Defendants violated Sections 17.46(a), 17.46(b)(9), and 17.46(b)(24) of the Texas Deceptive Trade Practices Act.

Count II: Misrepresentations Concerning the Use of Driving Data

100. Defendants falsely, expressly or by implication, misrepresented how they would use the data collected about their customers, including by making false and misleading statements that customers' information would be used to develop, enhance, provide, service, maintain, and improve the safety, security, and quality of GM's products, programs, and services, and for product research and marketing. In reality, General Motors also self-servingly used the vast amount of data it collected about its customers to derive a profit by repeatedly selling its customers' information to several different companies over the course of nearly a decade.

101. In doing so, Defendants violated Sections 17.46(a), 17.46(b)(9), and 17.46(b)(24) of the Texas Deceptive Trade Practices Act.

Count III: Misrepresentations Concerning the Sale of Driving Data

102. Defendants falsely, expressly or by implication, misrepresented their practice of sharing and selling customers' information, including by stating they would only "share" customers' information with certain categories of third parties.

103. In fact, Defendants entered into several unrelated agreements explicitly to sell customers' information, none of which involved marketing activities. Defendants never disclosed to customers that their information would be sold for other purposes.

104. In doing so, Defendants violated Sections 17.46(a), 17.46(b)(9), and 17.46(b)(24) of the Texas Deceptive Trade Practices Act.

Count IV: Misrepresentations Concerning Smart Driver and the Collection of Driving Data

105. Defendants falsely, expressly or by implication, misrepresented the purpose of the collection of data by Smart Driver as being for the customer's benefit, not other companies such as Insurers. Defendants' Smart Driver description stated it would provide customers with insights and feedback into their driving behavior and listed some of the "factors" used to calculate a customer's Driving Score.

106. In doing so, Defendants violated Sections 17.46(a), 17.46(b)(9), and 17.46(b)(24) of the Texas Deceptive Trade Practices Act.

Count V: Deceptive Techniques Used to Enroll Customers

107. Defendants used several false, misleading, and deceptive techniques to obtain customers' "consent" to Defendants' collection and sale of their data, including through its utilization of an aggressive onboarding program that included misrepresenting to customers that its dealership onboarding process was a pre-requisite to taking ownership of their vehicles.

108. In doing so, Defendants violated Sections 17.46(a), 17.46(b)(9), and 17.46(b)(24) of the Texas Deceptive Trade Practices Act.

Count VI: Deceptive Representations regarding Privacy Practices

109. Defendants purported to provide consumers with disclosures of their privacy practices, but utilized lengthy and confusing privacy statements that obfuscated Defendants' practices.

110. Defendants falsely, expressly or by implication, represented that customers would be able to exercise control over the sharing of their data with insurance providers when such was not the case.

111. In doing so, Defendants violated Sections 17.46(a), 17.46(b)(12), and 17.46(b)(24) of the Texas Deceptive Trade Practices Act.

TRIAL BY JURY

112. The State demands a jury trial and tenders the appropriate fee with this petition.

PRAYER FOR RELIEF

113. The State of Texas respectfully requests that this Honorable Court impose civil penalties on Defendants pursuant to Section 17.47(c) of the DTPA, which authorizes the Office of the Texas Attorney General's Consumer Protection Division to request a civil penalty to be paid to the State of Texas in an amount of: (1) not more than \$10,000 per violation; and (2) if the act or practice that is subject of the proceeding was calculated to acquire or deprive money or other property from a consumer who was 65 years of age or older when the act or practice occurred, an additional amount of not more than \$250,000.

114. The State of Texas further respectfully requests that this Honorable Court issue an order:

- (a) Declaring Defendants' conduct as described herein to be in violation of the DTPA;
- (b) Directing Defendants to delete or otherwise destroy all Driving Data obtained prior to the entry of any judgment by this Court, including any Driving Data in the possession of any third party;
- (c) Directing Defendants to make full restitution to all consumers who suffered a loss as a result of the acts and practices alleged in this Complaint and any other acts and practices proved by the State, pursuant to Section 17.47(d) of the DTPA; and

- (d) Permanently enjoining Defendants, their agents, employees, and all other persons acting on their behalf, directly or indirectly, from violating the DTPA, including by: (1) incorporating, employing, or otherwise using, directly or indirectly, any pattern or design that relates in any way to Driving Data, which causes, or is intended to cause, a consumer to act in a way that they would not absent the pattern or design, including mechanisms to obtain consent from consumers; and (2) collecting and selling Driving Data without providing customers with a clear and conspicuous notice of Defendants' practices and obtaining customers' express, informed consent.

115. The State of Texas further respectfully requests that this Honorable Court award the Office of the Texas Attorney General attorney's fees and costs of court pursuant to Texas Government Code Section 402.006(c), under which attorney's fees and costs of court are recoverable by the Office of the Texas Attorney General.

116. Lastly, the State of Texas respectfully requests that this Honorable Court grant any other general, equitable, and/or further relief this Court deems just and proper.

Respectfully submitted,

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

RALPH MOLINA
Deputy First Assistant Attorney General

JAMES LLOYD
Deputy Attorney General for Civil Litigation

RYAN S. BAASCH
Chief, Consumer Protection Division

/s/ Tyler Bridegan

TYLER BRIDEGAN
State Bar No. 24105530
ROBERTA H. NORDSTROM
State Bar No. 24036801
Assistant Attorneys General
Consumer Protection Division
808 Travis Street, Suite 1520
Houston, Texas 77002
Tyler.Bridegan@oag.texas.gov
Roberta.Nordstrom@oag.texas.gov

SUMMER R. LEE
State Bar No. 24046283
Assistant Attorney General
Consumer Protection Division
P.O. Box 12548
Austin, Texas 78711-2548
Summer.Lee@oag.texas.gov

Dated: August 13, 2024

ATTORNEYS FOR THE STATE

Automated Certificate of eService

This automated certificate of service was created by the eFiling system. The filer served this document via email generated by the eFiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Zeilic Contreras on behalf of Tyler Bridegan
Bar No. 24105530
zeilic.contreras@oag.texas.gov
Envelope ID: 90853104
Filing Code Description: Petition
Filing Description: Plaintiffs Original Petition
Status as of 8/13/2024 3:46 PM CST

Associated Case Party: State of Texas

| Name | BarNumber | Email | TimestampSubmitted | Status |
|-------------------|-----------|---------------------------------|----------------------|--------|
| Roberta Nordstrom | 24036801 | roberta.nordstrom@oag.texas.gov | 8/13/2024 3:13:10 PM | SENT |
| Summer Lee | 24046283 | summer.lee@oag.texas.gov | 8/13/2024 3:13:10 PM | SENT |
| Glenn Gallegos | | glenn.gallegos@oag.texas.gov | 8/13/2024 3:13:10 PM | SENT |
| Esther Chavez | | esther.chavez@oag.texas.gov | 8/13/2024 3:13:10 PM | SENT |
| Tyler Bridegan | | tyler.bridegan@oag.texas.gov | 8/13/2024 3:13:10 PM | SENT |

**Written Testimony
Of
Michael A. Moné, BSPHarm, JD, FAPhA
Principal, Michael A. Moné & Associates, LLC
On Behalf Of
Safelite Group, Inc.**

**Before The
Maryland Senate
Finance Committee**

Ensuring Marylanders' Access to Device Data

Submitted January 17, 2025

Thank you, Chairwoman Beidle, Vice Chairman Hayes, and Members of the Committee for inviting Safelite Group, Inc. (“Safelite”)¹ to submit this written testimony regarding the need to ensure Marylanders have easy access to and use of the personal data produced by their physical devices including vehicles they own/lease. Safelite shares the Committee’s goal of protecting Marylanders’ privacy, control, and use of their personal data.

Safelite believes that in a world of highly complex vehicles, where they not only move us from to place to place but also collect and create voluminous data about our driving behavior and the systems used to keep us safe in our travels, consumers and third-parties of their choice should be able to readily access data generated by their vehicle at no cost. In fact, such access is a matter of public safety as potential issues with our vehicles put occupants, other motorists, and bystanders at risk. Although these comments will speak primarily to vehicle data because that is Safelite’s area of expertise, the same principles also would hold true for other physical devices such as cellphones, tablets, computers, smart doorbells, in-home cameras, mobility aids, medical devices, and more.

As explained in more detail below, the Maryland Online Data Privacy Act of 2024 (“MODPA”) contains a mechanism for consumers to obtain access to personal data; however, this law contains ambiguities and limitations that prevent consumers from fully utilizing the benefit of their device data. Safelite encourages the Committee to conduct a study to assess areas for potential revision to the MODPA ensuring (i) device data that can be directly or indirectly linked to an identifiable person is clearly understood as personal data under MODPA, and (ii) consumers and their authorized service providers can access such data quickly and without cost.

Device Data is Personal Data

The MODPA enshrines the principle that consumers have the right to control their personal data. It defines personal data as “any information that is linked or can reasonably be linked to an identified or identifiable consumer.”¹ Vehicle data, including telematics data produced by the vehicle and diagnostic data such as fault codes, can be linked to an identified or identifiable consumer in multiple ways. Two scenarios help explain. First, imagine a consumer visiting a Safelite location to receive vehicle service. Safelite logs the consumer’s name and

¹ MD COML § 14-4601(w). Citations to MD COML are based on 2024 Maryland Laws Ch. 454 (H.B. 567).

contact information and the VIN of the vehicle to be serviced. The Safelite technician plugs a diagnostic scan tool into the vehicle and retrieves diagnostic data. Such diagnostic data is automatically associated with the VIN through the tool's software, or the technician manually associates it with the VIN in the customer record. Because the customer's name and contact information is associated with the VIN, and the VIN is associated with the diagnostic data, the diagnostic "can reasonably be linked" to that consumer. In a second scenario, when the consumer purchased the vehicle, the OEM received a report from the dealership identifying the purchaser, their contact information, and the VIN associated with the vehicle. As the vehicle is driven, telematics and diagnostic data of the vehicle is automatically collected by the OEM and related in its systems to the vehicle's VIN. As in the above scenario, because the OEM has the consumer's name and contact information in its database associated with the vehicle's VIN, and the collected vehicle data is associated with the VIN, such data is linkable to the consumer.

Some may argue that vehicle data associated with a VIN is not personal data because one may not know that the consumer it is believed to relate with was the individual driving the vehicle when the data was generated. This position simply misses the point. Regardless of who was driving the vehicle at the time it generated the data, if the data is associated with the VIN (or any other unique identifier tied to an individual), it reasonably can be, and most likely will be, linked to the consumer who is associated with the VIN. Put another way, the law does not specify which consumer the data must be associated with, only that it be capable of association with a consumer.

Accordingly, Safelite's position is that vehicle data is personal data. In fact, Safelite provides access to vehicle data it collects that is associated with a consumer when that consumer makes a verified request under their state's comprehensive privacy law to access their personal data. OEM privacy notices also often include vehicle data as a type of personal data, for example.

- FCA US – "...we collect and derive personal information through our Connected Services, including information about and your vehicle, as well as other users of your vehicle and the Services, such as vehicle usage and performance data, driving data, geolocation data, settings and presets, and features and services

accessed and used (including third party provided), and other information related to your use of our Connected Services.”²

- Ford Motor Co. – “Ford and Lincoln vehicles have systems that record data about how the vehicle is performing, how it is driven, where it is located, and the environment where it is operated. This data may be associated with a vehicle's unique identification number (“VIN”) or other identifiers, and VIN or the other identifiers may be linked to you.”³
- General Motors – “The types of Personal Information that GM collects about you when you interact with us include: ... information about your vehicle or information that is obtained from your vehicle that is linked to you or can be linked to you. For example, we may be able to link information to you from your vehicle, including license plate number and vehicle identification number (VIN), or vehicle status, including mileage, oil/battery status, ignition, window, door/trunk lock status, vehicle diagnostic information, EV charging and discharging and stationary energy storage details.”⁴

The same logic would apply to data generated by or derived from any physical device if such data is associated with a unique identifier that is connected to a consumer. Cellphones, computers, mobility aids, smart doorbells, medical devices, and others constantly generate data. Often data generated by or derived from these devices is tied to a unique identifier such as an IMEI, MAC address, or device ID. The unique identifiers frequently are, or can be, through matching with other data sets, tied to an identifiable consumer. Accordingly, data derived from these devices should also be treated as personal data under MODPA.

Explicitly clarifying that the MODPA treats device data that can be linked, directly or indirectly such as through association with a VIN or other identifier, to an identified or identifiable consumer would resolve any ambiguity and protect consumer rights.

² FCA US Privacy Policy, available at https://www.chrysler.com/crossbrand_us/privacy (accessed 01-10-2025).

³ Ford Motor Company US Privacy Notice, available at <https://www.ford.com/help/privacy/#USprivacynotice> (accessed 01-10-2025).

⁴ General Motors U.S. Consumer Privacy Statement, available at <https://www.gm.com/privacy-statement> (accessed 01-10-2025).

Timely No-Cost Access is Vital to Preserve Consumer Interests

The MODPA allows consumers to request access to their personal data from the data controller for free once per twelve-month period.⁵ Generally, data controllers make available a web form and/or toll-free number through which a consumer may make such requests under other states' privacy laws, and one would expect a similar approach under MODPA. The law allows the data controller 45 days, plus one additional 45-day extension under certain circumstances, to provide access to the personal data.⁶ If the data controller denies the request necessitating an appeal by the consumer, the controller may take up to 60 days to fulfill the appeal.⁷ This means it may take a consumer up to 150 days from when they initially make their request to receive access to their personal data.

Although 150 days may be sufficient for obtaining personal data out of curiosity or a desire to archive historical information, in the context of obtaining vehicle or other device data it is unacceptably long. If the consumer needs to access their vehicle data to provide it to their authorized service technician in connection with a vehicle repair, that repair is urgent and failing to complete it may render the vehicle inoperable or unsafe⁸. For example, driving with a chipped or cracked windshield may increase the risk of sudden catastrophic windshield failure that could not only result in harm to the vehicle occupants, but also in a loss of control of the vehicle potentially injuring other motorists or bystanders. Delaying this repair through the passage of time or by limiting who can make such repair, thereby creating a bottleneck, is a risk to public safety, and any arguments contrary to such position are inapposite to consumer wellbeing.

Additionally, because much of the vehicle data is stored on-board the vehicle, the OEM may not be able to provide it by the traditional access request process necessitating a method for the consumer or their authorized agent to access the on-board systems that store the data and retrieve it. OEMs may unfairly erect technological and/or financial barriers to accessing this on-board data. When a vehicle service provider seeks to retrieve diagnostic data from a vehicle, it can do so with physical access to the vehicle and a specialized tool that can read and report the

⁵ MD COML §§ 14-4605(b)(2); 14-4605(b)(4).

⁶ MD COML § 14-4605(e)(1)-(2).

⁷ MD COML § 14-4605(f)(3).

diagnostic data. However, certain types of diagnostic data and systems that generate such data, such as those related to safety system recalibration following a windshield replacement, require OEM authentication or access to OEM software to access the on-board data and systems.

OEMs typically charge fees for authentication or access to their software, either directly or by payments to third-party providers that can provide access due to their relationships with OEMs. In 2024, Safelite paid one third party provider over \$9,000,000 on such authentication and access. Because of Safelite's scale, it is able to absorb these costs to lower the impact on consumers, but such fees could become prohibitively expensive. In Safelite's experience these fees can be upwards of -\$100 per vehicle. Such costs may also prevent small repair shops from offering the services because they are not capable of absorbing those costs and remain competitive, or cannot afford upfront setup fees, annual licensing or purchasing specialized tools that may be required. These costs could make it difficult for consumers, particularly those in smaller towns or remote areas without immediate access to a franchised dealership, to readily obtain necessary repairs that are convenient and affordable. Additionally, these fees and access as a whole are completely subject to the whims of the OEMs, and they could unilaterally increase fees, or limit access to preferred authorized service providers, or block access entirely if they so choose in the future. More critically, the true question is why should a consumer or their authorized service provider be required to pay fees at all to access the consumer's own data on the consumer's own device?

The MODPA also requires that the consumer's personal data, if it is automatically processed, be provided to the consumer in a "portable and, to the extent technically feasible, readily usable format that allows the consumer to easily transmit the data to another controller without hinderance."⁹ As evidenced by this provision in the current law, one of the MODPA's goals is to ensure that consumers may easily make their personal data available to third parties of their choosing without interference. Paywalls and other manufacturer restrictions on access and use of device data clearly inhibit this goal. Safelite also is concerned that device manufacturers may argue that it is not technically feasible to provide the data in a readily usable format because they have not developed technical means to do so. This lack of investment on the part of a manufacturer should not be a barrier to consumer access and use of their device data, and

⁹ MD COML §§ 14-4605(b)(5).

manufacturers should be obligated to invest in systems that allow export in a readily usable format and easy transmission to the consumer or a third party of their choosing.

Study and Legislative Action

Safelite encourages the Committee to launch a study to answer a few questions:

1. What can be done to ensure that Marylanders have ~~easy~~ access for the purpose of vehicle repair access to their personal data that is generated from, or stored upon, their personal devices without interference from device manufacturers along with the ability to easily transfer that personal data to a third party they authorize?
2. In situations where access is time-sensitive, such as in connection with repair of the device, what legislative changes are needed in the future to ensure Marylanders can access their data and associated systems in real time or near real time?
3. Among the states that have data privacy laws, how are they addressing the issue of the right to repair?

Safelite has considered changes to the MODPA to achieve these goals and believes that legislative action to create an express right of consumers and their authorized service providers to timely cost-free access to their personal data generated by or stored on their physical devices is appropriate. When access is time-sensitive, such as in the case of a need to repair the device, the manufacturer should provide a cost-free real-time access method.¹⁰ After all, this data is derived from or located on the consumer's device and the consumer should be able to control and fully utilize their data to their benefit. Safelite would be pleased to provide further input during the study process.

Conclusion

Safelite appreciates the Committee's attention to this issue and the ability to provide its perspective on how to ensure Marylanders have ~~easy~~ access to data generated by their devices/automobiles they own for the purposes of diagnostic and repair. The changes Safelite is

¹⁰ The MODPA's one per twelve-month period limit on access requests should not apply to the cost-free real-time access method because it will certainly be automated and, therefore, each request will not materially increase the manufacturer's compliance costs. Additionally, consumers can unfortunately experience multiple instances of vehicle damage within a year necessitating exercising this right each time.

asking to consider are not limited to glass repair, but its implications are much broader than glass and impacts the entire vehicle repair industry. Together, we stand ready to respond to any questions the Committee may have on this topic.

Appendix A

Michael A. Moné, BSPHarm, JD, FAPhA
Principal, Michael A. Moné & Associates, LLC

As a licensed pharmacist and lawyer, Moné has served in a variety of roles in private and public practice of law and pharmacy. Michael led the Kentucky Board of Pharmacy for eight years where he developed statewide public health policy and oversaw all investigative efforts for the agency, including responsibilities for addressing patient and consumer data and health privacy concerns. He also served as an attorney for the Florida Board of Pharmacy and as an Assistant Attorney General in Florida as the general counsel for the Boards of Chiropractic, Osteopathic Medicine, Veterinary Medicine and Pilot Commissioners, where in these roles' privacy concerns of patients and consumers were again a component of Michael's responsibilities.

Most recently prior to his transition to the position of Principal, Michael A. Mone & Associates, LLC, Michael was Senior Legal Counsel for CVS Health where he represented and advised business units in their interactions with pharmacy providers and government agencies. In this role, patient and consumer health and data privacy were addressed. Michael also served as Vice President-Associate General Counsel/Regulatory, where he provided regulatory counsel to various Cardinal Health business units and represented Cardinal Health before state regulatory agencies, including participation in Attorneys General meetings where he served as a subject matter expert in regulatory matters, including patient and consumer health and data privacy.

Moné has held leadership roles within many industry associations, including the National Association of Boards of Pharmacy, Ohio State Board of Pharmacy, Accreditation Council for Pharmacy Education, U.S. Pharmacopeia, American Pharmacists Association and Florida Pharmacy Association. He also served on the Kentucky Governor's Task Force on Controlled Substance Abuse and the Attorney General's Task force to develop KASPER, the Kentucky All Schedule Prescription Electronic Reporting System, which tracks controlled substance prescriptions dispensed within the state to stop abuse, misuse, diversion, and illegal sale of prescription drugs.

He attended the University of Florida where he received both his Juris Doctorate and Bachelor of Science in Pharmacy.



ALLIANCE
FOR AUTOMOTIVE
INNOVATION



Senate Finance Committee

Briefing: Consumer's Right to Repair Motor Vehicles

Wayne Weikel, Vice-President of State Affairs

January 22, 2025



Who We Are

AESC



• APTIV •



Autoliv

BMW GROUP

BOSCH

DENSO



HONDA

HYUNDAI

INEOS Automotive



ISUZU



LG

LUMINAR

MAGNA



McLaren



Mercedes-Benz



nuro

Panasonic

PORSCHE

Qualcomm



SAMSUNG SDI



STELLANTIS



TEXAS INSTRUMENTS

TOYOTA

Uber



VINFAST

VOLKSWAGEN
GROUP OF AMERICA

VOLVO

ZOOX

Topline Points

Automakers Support Right to Repair

1. All information needed to diagnose and service a vehicle is available to repairers
2. Consumers benefit from a competitive marketplace full of automotive repair options
3. Automakers work with repairers in service to shared customers



Early Right to Repair Movement

Started in 1996 with new OBDII vehicle architecture

Lots of state and federal legislation filed

Ultimately, led to so-called “Dorgan Letter” in 2002

- Automakers agreed to provide both repair information and diagnostic tools to repairers, in **same manner as available to dealers**



Ballot Question and National MOU

2012 Ballot Question in Massachusetts Codified Dorgan Letter

- Added EPA “reasonableness” standard to cost of tools and repair info
- Closed “loophole” on telematics data
- Required a standardized interface option

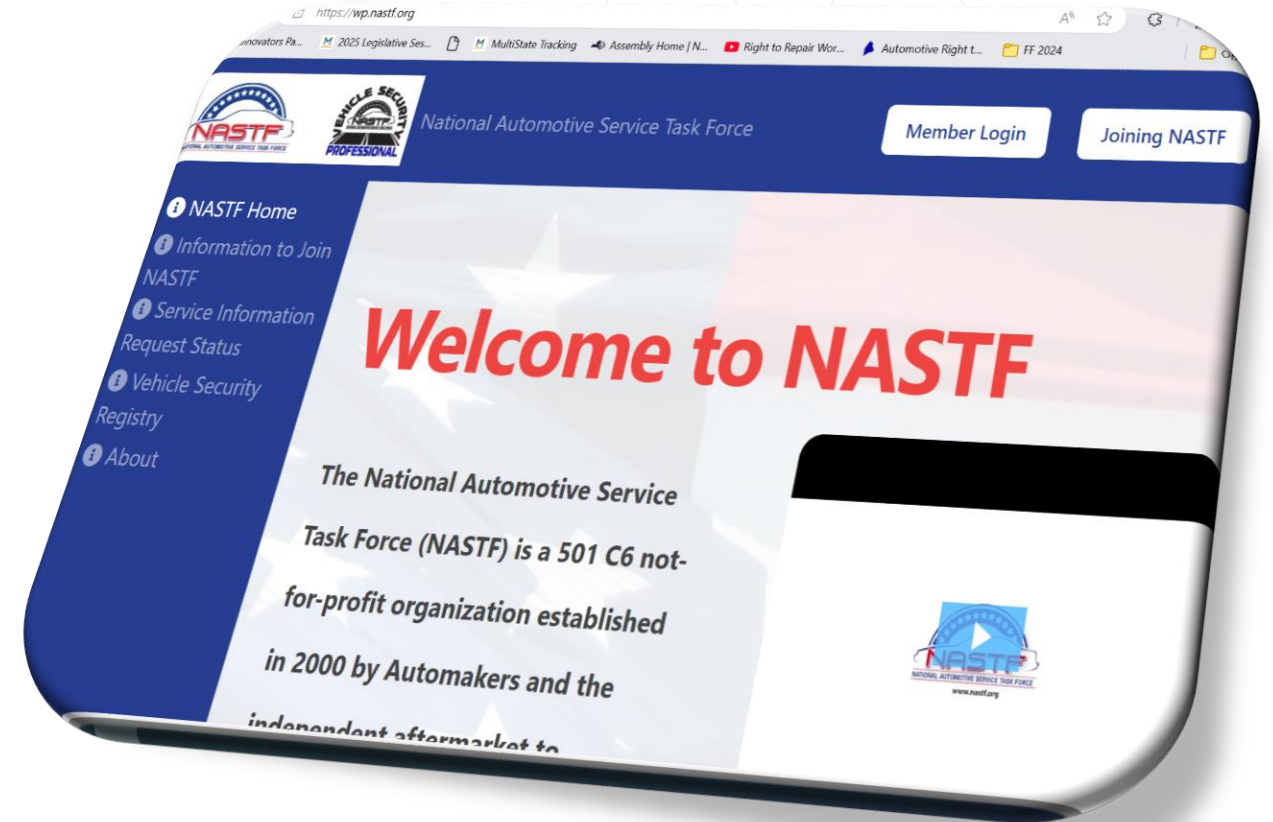
2014 MOU Signed to Apply Massachusetts Law Nationally



Resources for Repairers

National Automotive Service Task Force

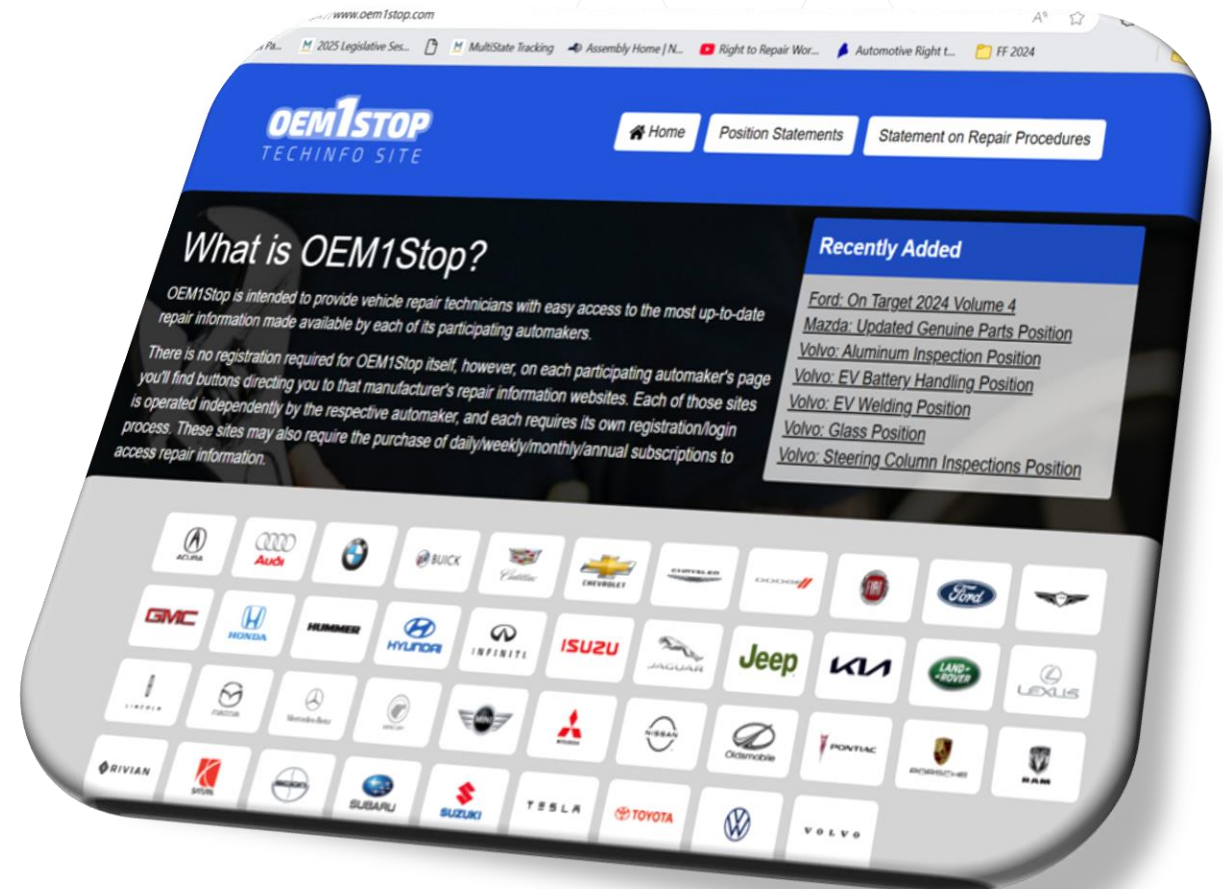
- ✓ Created and funded by automakers in 2000
- ✓ Provides venue to identify and resolve any gaps in repair information



Resources for Repairers

www.OEM1Stop.com

- ✓ Created and funded by automakers
- ✓ Provides repairers with single point of access for repair data
- ✓ Links directly to automaker repair data websites



Automakers are the Gold Standard for R2R

Federal Trade Commission 2021 “Nixing the Fix” Report

For any manufacturing sector interested in creating a self-regulatory mechanism for expanding repair options, the experience of the automobile industry provides some guidance... a Memorandum of Understanding that had the effect of creating a **broad, if not complete, right to repair in the automotive industry across the United States.**” Page 45.

“While the car manufacturing industry has taken important steps to expand consumer choice, other industries that impose restrictions on repairs have not followed suit. Page 6.

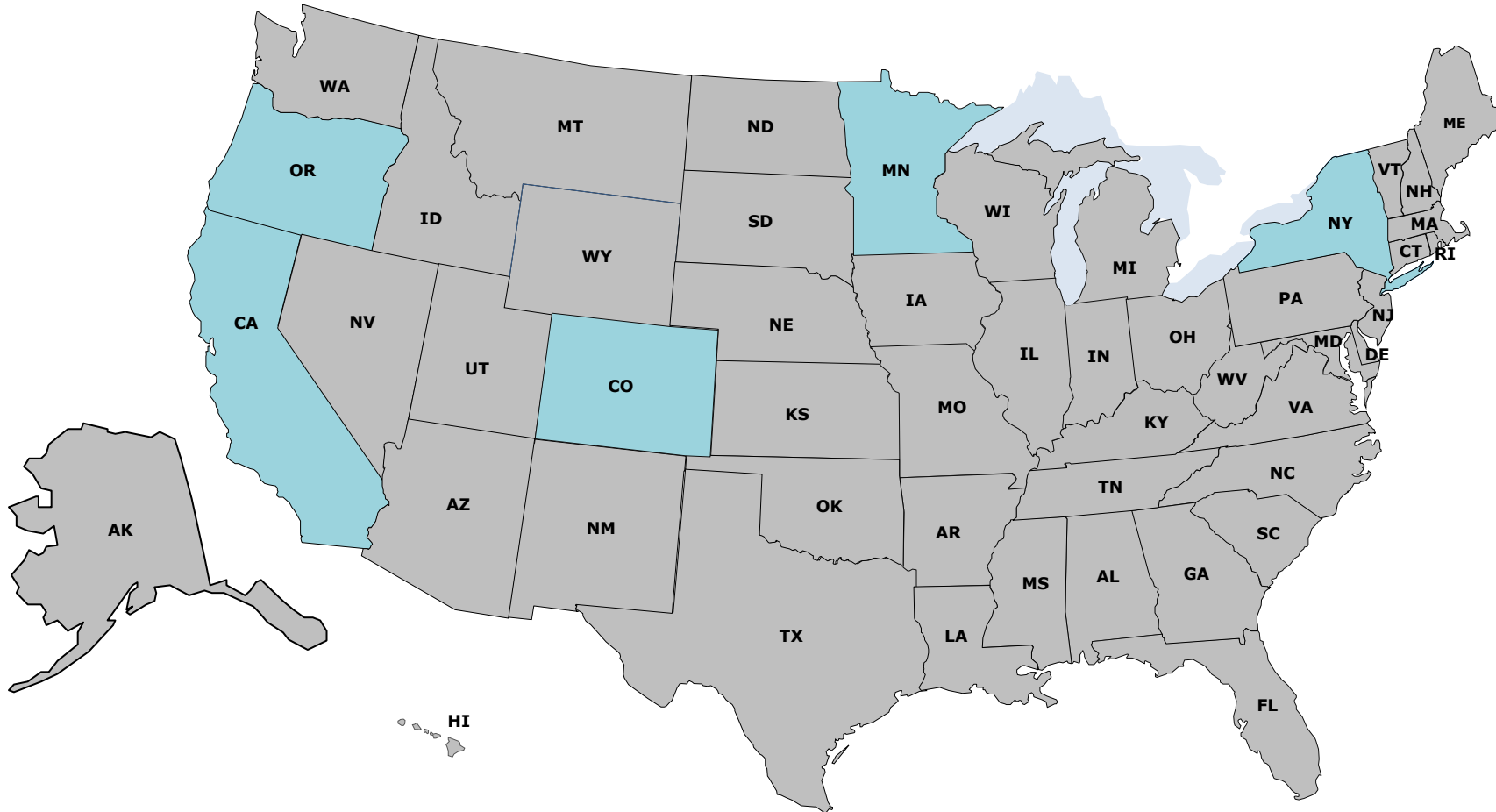
Automakers are the Gold Standard for R2R

Kyle Wiens, CEO of iFixit - Leader in the National R2R Movement Washington Post Op/Ed

In some sectors, notably the automotive industry, independent repair shops are thriving. The ability of individuals and third-party shops to obtain the same electronic-diagnostic information available to dealers was codified in a 2013 Massachusetts law...

Thanks to that agreement, you have the choice to get your car fixed at a local shop or at the dealership. Nationwide, independent mechanics perform about 70 percent of all automotive repairs. That competition keeps prices reasonable while also stabilizing car insurance rates.”

Automakers are the Gold Standard for R2R



5 States have
passed
“Digital” Right
to Repair Laws

--

All Exclude
Automobiles

Automakers are the Gold Standard for R2R

Why?

Because automakers already do what they want every other industry to start doing!

Making available the parts, tools, and repair information needed to complete repairs.

Automobiles

Renewed National Agreement in 2023



Key Takeaway

Automakers Know Repair Experience Matters to Brand Loyalty!

Renewed National Agreement in 2023

Agreement between:

Alliance for Automotive Innovation
Automotive Service Association
Society of Collision Repair Specialists

Key Tenets:

Access to diagnostic and repair information, including:

- ✓ Access to telematics data, if needed
- ✓ All propulsion types – ICE, EVs, Hybrids, & Fuel Cell
- ✓ Access to tools and 3rd party tool manufacturers
- ✓ Assessment of training options available
- ✓ Working group created to solve any gaps found
- ✓ Industry panel created to talk about new technologies when they come into the marketplace



**So, if things are so great,
why do we keep hearing
about Right to Repair in
the auto sector?**



Who is Paying the Bills?

Not Every “Repairer” Group Represents Repairers

Massachusetts Right to Repair Coalition

2020 - Ballot Question on Remote Vehicle Data Access

Who is Paying the Bills?

Not Every “Repairer” Group Represents Repairers

Massachusetts Right to Repair Coalition

2020 - Ballot Question on Remote Vehicle Data Access

\$24,862,978 - raised for campaign

99.997% - from out-of-state part manufacturers and retailers

Who is Paying the Bills?

Not Every “Repairer” Group Represents Repairers

Maine Right to Repair Coalition

2023 - Ballot Question on Remote Vehicle Data Access

Who is Paying the Bills?

Not Every “Repairer” Group Represents Repairers

Maine Right to Repair Coalition

2023 - Ballot Question on Remote Vehicle Data Access

\$4,920,000 - raised for campaign

99.999% - from out-of-state part manufacturers and retailers

Who is Paying the Bills?

Not Every “Repairer” Group Represents Repairers

Federal CAR Coalition Members

Aftermarket Parts:

AutoZone; ABPA; CAPA; LKQ

Insurers:

Allstate; Farmers; Amica, APCIA

Parts Platforms:

Carparts.com; Partstrader.com



With Whom Did We Partner? Repairers.

Automotive Service Association

ASA is the **largest and oldest national organization** committed to protecting the automotive repair industry with ONE VOICE.

Our members own and operate automotive mechanical and collision repair facilities responsible for the majority of all post-warranty, repair services in the United States.

ASA advocates for the interests of its members and their customers in Washington, D.C. The education, resources, and services ASA provides empowers its members in all 50 states to remain trusted stewards of mobility in their communities.

www.ASAShop.org

Society of Collision Repair Specialists

Through our direct members and affiliate associations, SCRS proudly represents over **6,000 collision repair businesses and 58,500 repairers** who work to repair collision-damaged vehicles.

Since 1982, SCRS has served as the largest national trade association **solely dedicated to the collision repair facilities** across North America.

Since its formation, SCRS has provided repairers with an audible voice, and an extensive grassroots network of industry professionals who strive to better our trade.

www.SCRS.com

Topline Points to Remember

Automakers Support Right to Repair

1. All information needed to diagnose and service a vehicle is available to repairers
2. Consumers benefit from a competitive marketplace full of automotive repair options
3. Automakers work with repairers in service to shared customers



Thank You

Questions?





ALLIANCE FOR AUTOMOTIVE INNOVATION

The background of the slide is a blurred, dark blue-tinted image of a highway with traffic, viewed from the driver's perspective. A side-view mirror is visible in the lower right foreground. On the left side, there are three overlapping teal arrow shapes pointing to the right.

Telematics and Cybersecurity

OEM Cloud-Based Server Model



Massachusetts Ballot Question Model



Open Telematic Access a Cybersecurity Risk

National Highway Traffic Safety Administration

“A malicious actor here or abroad could utilize such open access to remotely command vehicles to operate dangerously, including attacking multiple vehicles concurrently.”

“... NHTSA has grave concerns with any proposed policy that would effectively prohibit wireless access controls in motor vehicles sold in the United States. This would raise substantial safety risks for American families.”

Bryan Reimer, Ph.D – MIT, Center for Transportation

“... What worries me the most, is that the bill will accelerate society toward a major cyber terrorism threat... If bills such as those proposed were to be enacted, I have advised manufacturers to cease selling products in the state. The cyber terrorism risks of an open network are truly too large.”