U.S. Department of Transportation
National Highway Traffic Safety Administration

NHTSA

June 13, 2023

Ann Marie Dias-Lebrun
Assistant General Counsel
BMW of North America, LLC
annmarie.dias-lebrun@bmwna.com

David M. Wertheim
Vice President & General Counsel
Ferrari North America, Inc.
david.wertheim@ferrari.com

Natalia Medley
Senior Counsel
Fisker Group Inc.
nmedley@fiskerinc.com

Christina Michaels
Attorney
Ford Motor Company
cmicha18@ford.com

Suzanne Miklos
Vice President - Global Product Safety & Systems
General Motors LLC
suzanne.miklos@gm.com

Jack Alden
Senior Counsel
American Honda Motor Co.
jack_alden@na.honda.com

Jason Erb
Chief Legal Officer
Vice President, Legal
Hyundai Motor America
jerb@hmausa.com

Ramsey Ong
General Counsel
Jaguar-Land Rover
rong2@jaguarlandrover.com

Jeremy Close
Attorney
Kia Motors America
jclose@kiausa.com

Charles Kim
Assistant General Counsel
Mazda North American Operations
ckim1@mazdausa.com

Nick Ball
General Counsel
McLaren Automotive Incorporated
nick.ball@mclaren.com

Anthony Zeph
Associate General Counsel
Mercedes-Benz North America
Anthony.Zeph@mbusa.com

Katherine Knight
Vice President, General Counsel
Mitsubishi Motors North America, Inc.
katherine.knight@na.mitsubishi-motors.com

Emily Landry
Assistant General Counsel
Nissan North America, Inc.
emily.landry@nissan-usa.com

George Feygin
General Counsel
Porsche Cars North America, Inc.
george.feygin@porsche.us

Nancy Bell
General Counsel
Rivian Automotive, LLC
nbell@rivian.com

Alan Degraw
Senior Counsel
Stellantis
alan.degraw@stellantis.com

Michael Carroll
Associate General Counsel
Subaru of America
mcarro@subaru.com

Eric Williams
Associate General Counsel, Regulatory
Tesla, Inc.
erwilliams@tesla.com

Kimberly Utevic
Assistant General Counsel
Toyota Motor North America
kim.udovic@toyota.com

Brian Kapatkin
Corporate Counsel
Volkswagen Group of America, Inc.
brian.kapatkin@vw.com

Robert Sullivan
Counsel
Volvo Car USA, LLC
robert.sullivan@volvocars.com

Dear Counsel for Vehicle Manufacturers:

The National Highway Traffic Safety Administration (NHTSA) is sending this letter to advise vehicle manufacturers of their obligations under the National Traffic and Motor Vehicle Safety Act (Safety Act), 49 C.F.R. Chapter 301, in light of a Massachusetts law that NHTSA believes poses significant safety concerns. That law, previously known as SD645 and now codified at Chapter 93K of the Massachusetts General Laws (the Data Access Law), requires open remote access to vehicle telematics.[1] As explained below, the Data Access Law conflicts with and therefore is preempted by the Safety Act.

While NHTSA has stressed that it is important for consumers to continue to have the ability to choose where to have their vehicles serviced and repaired, consumers must be afforded choice in

[1] NHTSA understands that Massachusetts stated its intent to enforce the law beginning on June 1, 2023. *Alliance for Automotive Innovation v. Campbell*, Case No. 1:20-cv-12090, Dkt. No. 330 ("Notice of Intent to Terminate Non-Enforcement Stipulation") (D. Mass) (hereinafter "Notice of Intent").

a manner that does not pose an unreasonable risk to motor vehicle safety.[2] In this case, NHTSA previously described its serious safety concerns with the Data Access Law's requirement of open remote access in a filing in pending federal district court litigation that challenges the law. *Alliance for Automotive Innovation v. Campbell*, Case No. 1:20-cv-12090, Dkt. No. 202 (D. Mass) ("United States' Statement of Interest").[3] The open remote access to vehicle telematics effectively required by this law specifically entails "the ability to send commands."[4] Open access to vehicle manufacturers' telematics offerings with the ability to remotely send commands allows for manipulation of systems on a vehicle, including safety-critical functions such as steering, acceleration, or braking, as well as equipment required by Federal Motor Vehicle Safety Standards (FMVSS) such as air bags and electronic stability control. A malicious actor here or abroad could utilize such open access to remotely command vehicles to operate dangerously, including attacking multiple vehicles concurrently.[5] Vehicle crashes, injuries, or deaths are foreseeable outcomes of such a situation.

Vehicle manufacturers appear to recognize that vehicles with the open remote access telematics required by the Data Access Law would contain a safety defect. Federal law does not allow a manufacturer to sell vehicles that it knows contain a safety defect. *See* 49 U.S.C. §§ 30112(a)(3); 30118(c)(1). Furthermore, as you are aware, the Safety Act imposes an affirmative obligation on vehicle manufacturers to initiate a recall of vehicles that contain a safety defect. 49 U.S.C. § 30118(c).

Given the serious safety risks posed by the Data Access Law, taking action to open remote access to vehicles' telematics units in accordance with that law, which requires communication pathways to vehicle control systems, would conflict with your obligations under the Safety Act.[6] "The purpose of the Safety Act . . . is not to protect individuals from the risks associated with defective vehicles only after serious injuries have already occurred; it is to prevent serious

---

[2] To ensure consumers have adequate access to repair facilities, a 2014 Memorandum of Understanding (MOU) already provides secure access to vehicle telematics to independent repair facilities nationwide. *See* MOU (Jan. 15, 2014) *available at* https://www.autocare.org/docs/default-source/government-affairs/r2r-mou-and-agreement-signed.pdf.

[3] *See also* Letter from James Owens, Deputy Administrator, NHTSA, to Massachusetts's Joint Committee on Consumer Protection and Professional Licensure (Jul. 20, 2020) *available at* https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa_testimony_in_response_to_ma_committee_letter_july_20_2020.pdf.

[4] Mass. Gen. Laws 93K § 2(f).

[5] As NHTSA has previously stated: "Wireless interfaces into vehicle systems create new attack vectors that could potentially be remotely exploited. Unauthorized wireless access to vehicle computing resources could scale rapidly to multiple vehicles without appropriate controls." *Cybersecurity Best Practices for the Safety of Modern Vehicles* at 15 (Sept. 2022), *available at* https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf.

[6] *See, e.g.*, NHTSA Recall No. 15V-461, *available at* https://static.nhtsa.gov/odi/rcl/2015/RCLRPT-15V461-9313.PDF; NHTSA Recall No. 15V-508, *available at* https://static.nhtsa.gov/odi/rcl/2015/RCLRPT-15V508-8738.PDF.

injuries stemming from established defects before they occur." *United States v. Gen. Motors Corp*., 565 F.2d 754, 759 (D.C. Cir. 1977).

NHTSA is aware that certain vehicle manufacturers have stated an intent to disable vehicle telematics, presumably to avoid the application of the Data Access Law to their vehicles.[7] This measure has its own adverse impacts on safety. For example, telematics-based safety features could facilitate better emergency response in the event of a vehicle crash. Telematics data can also be an important source of information for safety oversight and field performance monitoring by the authorities and vehicle manufacturers. NHTSA often utilizes telematics data in its investigations, and the inability to obtain these data from vehicles with this capability undermines the agency's ability to fully examine safety-related issues. In addition, some vehicle manufacturers have the ability to fix safety problems by remedying recalls through vehicle telematics, which will be lost if those systems are disabled. Manufacturers should assess the impacts of any planned actions on roadway safety comprehensively.

We appreciate your attention to this important safety matter and trust you will give your highest priority to ensuring motor vehicle safety. Because the Safety Act conflicts with and therefore preempts the Data Access Law, NHTSA expects vehicle manufacturers to fully comply with their Federal safety obligations.

Sincerely,

KERRY E KOLODZIEJ

Digitally signed by KERRY E KOLODZIEJ
Date: 2023.06.13 12:47:08 -04'00'

Kerry Kolodziej
Assistant Chief Counsel
for Litigation and Enforcement

CC:

Robert E. Toone
Assistant Attorney General
Commonwealth of Massachusetts
robert.toone@mass.gov

Jessica Simmons
Assistant General Counsel
Alliance for Automotive Innovation
jsimmons@autosinnovate.org

[7] Notice of Intent.