IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW

PARTIES' JOINT SUBMISSION REGARDING
TEXTUAL INTERPRETATIONS OF DATA ACCESS LAW

In accordance with the Court's September 1, 2022, September 14, 2022, and September 22, 2022 orders, Plaintiff Alliance for Automotive Innovation ("Plaintiff" or "Auto Innovators") and Defendant Attorney General Maura Healey ("Defendant" or "Attorney General") hereby submit this document summarizing the parties' respective positions on textual interpretation of the Data Access Law.

I. Introduction

On September 6, 2022, the Attorney General's counsel provided a draft document listing her interpretation of key terms in the Data Access Law and left a placeholder for Auto Innovators to set forth its positions, including whether it agrees with the Attorney General's interpretation of each term or believes that the term should be interpreted differently. On September 22, 2022, Auto Innovators provided its response to counsel for the Attorney General and listed additional terms in the Data Access Law for which it requested the Attorney General's interpretation. After additional exchanges of drafts and a meet-and-confer discussion, the parties adapted that document into the

submission below, which describes the parties' interpretations of key statutory terms and indicates whether the parties agree or disagree on those particular terms.

Auto Innovators' Additional Statement: Consistent with the Court's prior order, Auto Innovators intended in its responses to "exchange views" with the Attorney General in an attempt to "come to agreement" regarding the meaning of the Data Access Law. *See* Sep. 1, 2022 Tr. 23:2-3. Auto Innovators has supplemented its responses to provide certain citations to the record in response to the Attorney General's citations. In providing its responses, Auto Innovators does not waive the position it took at trial regarding the interpretation of the language of the Data Access Law, which interpretation was and will be subject to briefing and evidentiary submissions before, during, and after the trial in this action.

Attorney General's Additional Statement: The Attorney General will defend her textual interpretations in her forthcoming brief, but because Auto Innovators' response includes not just its textual interpretation of the terms in the Data Access Law but also legal argument, disclaimers, and discussion of implications for implementation, the Attorney General briefly responds to those arguments here.

II. Interpretation of Terms in Section 2

Section 2 of the Data Access Law provides that:

> motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless that authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.

G.L. c. 93K, § 2(d)(1).

A. "Motor vehicle"

The parties agree on the definition of this term.

- Auto Innovators' position: The term "motor vehicle" means any "vehicle, originally manufactured for distribution and sale in the United States, driven or drawn by mechanical power and manufactured primarily for use on public streets, roads and highways," with certain exceptions set forth in Mass. G.L. c. 93K, § 1. The definition does not exclude any particular vehicle propulsion system.

- Attorney General's position: The term "motor vehicle" means any "vehicle, originally manufactured for distribution and sale in the United States, driven or drawn by mechanical power and manufactured primarily for use on public streets, roads and highways," with certain exceptions set forth in Mass. G.L. c. 93K, § 1. This definition includes cars powered by internal combustion engines and electric cars.

B. "Access to vehicle on-board diagnostic systems" and "Access to vehicle networks and their on-board diagnostic systems"

The parties do not agree on the definition of this term.

- Auto Innovators' position:

  - The term "vehicle networks" refers to all of the electronic networks of the vehicle, which include CAN buses connecting ECUs.

  - The term "on-board diagnostic system" refers to a vehicle's internal computer system that monitors and reports vehicle performance issues.

  - The term "access" refers to an ability to interface with a vehicle system.

  Auto Innovators agrees with the Attorney General that, at a minimum, the interface entails obtaining data *from* the vehicle for the purposes of diagnosis, repair, and maintenance. However, Auto Innovators understands that the proponents of the Data Access Law envisioned that access includes the ability to send commands to the vehicle. Indeed, even "reading" data requires sending such commands. Therefore, taken together, "access to vehicle networks and their on-board diagnostic systems" means the ability to read and send commands to vehicles' electronic networks and internal computer systems.

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that (a) "access" would not necessarily require the person receiving such access to write data or send commands to the vehicle, and (b) the term "vehicle networks" does not include any electronic networks beyond those included within vehicles' on-board diagnostic systems (as the AG suggested in its interrogatory responses (*see* Tr. Ex. 30 at 3)), that may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular

provision/aspect of the Data Access Law. However, even that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular provision, and the Data Access Law as a whole, and in any event compliance with the statute as interpreted in this way—taken together with the statute's other requirements—would still take years to accomplish.

Finally, in response to the Attorney General's comment below, Auto Innovators notes that the evidence at trial established that OEMs could not provide the requisite "access" without compromising vehicle cybersecurity, and various prerequisites to such "access" do not currently exist. *See generally* Plaintiffs' Post-Trial Proposed Findings of Fact ("Pl. PFOF") and Conclusions of Law ("Pl. PCOL"), ECF No. 233, at Pl. PFOF ¶¶ 108-20.

- Attorney General's position: The term "access to vehicle networks and their onboard diagnostic systems" means access for obtaining data related to the purposes of diagnosis, repair, and maintenance.

  Contrary to Auto Innovators' argument, the evidence at trial established that "access to vehicle networks and their on-board diagnostic systems" can be provided in a way that does not compromise cybersecurity and which can be implemented in a timely manner. *See* Attorney General's Proposed Revised Substitute Findings of Fact and Conclusions of Law (hereinafter "AG Rev. FF"), ECF No. 232 ¶¶ 172-96.

C. "Standardized" and "Standardized across all makes and models sold in the Commonwealth"

The parties agree on the definition of this term, but disagree about what this definition requires and about OEMs' ability to comply with those requirements.

- Auto Innovators' position:
  - "Standardized" means to follow a common and well-documented means of performing a necessary action.
  - "Standardized across all makes and models sold in the Commonwealth" means that the relevant "access" and "authorization system" must be the same across all vehicles sold in the Commonwealth, regardless of manufacturer. Such standardization currently does not exist.

  Notwithstanding Auto Innovators' understanding of the law as described above, if the Court determines that "standardized across all makes and models sold in the Commonwealth" refers only to standardization across specific OEMs' makes and models, that may facilitate OEMs' ability to develop authorizations systems that would reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular

provision/aspect of the Data Access Law. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular provision or the Data Access Law as a whole. Further, that "standardization" will take years to accomplish, even if the standardization applies only across specific OEMs' makes and models, rather than across *all* OEMs' makes and models. "Standardization" across all OEMs would take even longer time, as it would require the entire auto industry to agree (with input not only from OEMs, but also other industry players and government regulators) upon a specific "standard" before that standard could be incorporated into vehicle designs. *See, e.g.*, Pl. PFOF ¶¶ 14-16, 104, 114-16 (describing lack of standardized authorization); June 14 Tr. 214:3-9, June 15 Tr. 24:24-26:7, 27:16-18, 97:1-7, 101:8-16 (same); Smith Aff. ¶¶ 49-51, 125-26, 147-48 (describing use of OEM-specific OBD-II ports and codes and "gap in standardization"); Ex. 27 at 3 (no standardized authorization exists). Moreover, "standardization" across all OEMs increases the cybersecurity attack surface and risk exponentially. *See, e.g.*, Bort Aff. ¶¶ 64-65; Chernoby Aff. ¶ 72; Tierney Aff. ¶¶ 92, 108-10.

- Attorney General's position: The term "standardized" means following a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating.

  The term "standardized across all makes and models sold in the Commonwealth" in Section 2 of the Data Access Law is not limited to the makes and models of a particular manufacturer, whereas the standardization requirement in Section 3 of the Data Access Law is so limited.

  Contrary to Auto Innovators' argument, the evidence at trial established that standardization can be accomplished in a manner that does not compromise cybersecurity and which can be done in a reasonable time, so long as the OEMs actually make an effort to implement the Data Access Law's requirements. *See* AG Rev. FF ¶¶ 46-49, 176-96. To the extent that Auto Innovators argues that "'[s]tandardization' across all OEMs exponentially increases the cybersecurity risk" by limiting "OEMs' ability to develop authorization systems that would reduce the loss of cybersecurity protections that would otherwise occur through compliance with this particular provision/aspect of the Data Access Law," the evidence at trial disproved this argument, as it established that standardization of authorization systems can be accomplished without decreasing cybersecurity, and, in fact, many OEMs (like Toyota) allow access to their on-board diagnostic systems without requiring any manufacturer authorization at all. *See* AG Rev. FF ¶¶ 172-74; Tr. II:108-19, 129, 217-18; Potter Aff. ¶¶ 44-48, 56.

D. "Authorization" and "Authorization System"

The parties do not agree on the definition of this term.

- Auto Innovators' position: "Authorization" means an actor's role or what it is and is not permitted to do on a system.

  Auto Innovators agrees with the Attorney General's position (below) that the term "authorization" encompasses an actor's role or what it is and is not permitted to do on a system. However, Auto Innovators disagrees that "[a]uthorization is distinct from authentication." *See generally* Pl. PCOL ¶¶ 59-60; Romansky Aff. ¶ 20; June 14 Tr. 210:24-211:3, 249:15-19. There can be no restrictions on what an actor "is and is not permitted to do on a system" (*i.e.*, authorization) without "confirmation of the identity of an individual, user, or other actor" (*i.e.*, authentication). Therefore any "authorization" and "authorization system" necessarily includes a means of authenticating the identify of an individual, user, or other actor. Accordingly, the effect of the "authorization" language is to exclude OEMs from any authorization or authentication process for access to on-board diagnostic systems and vehicle networks. *See, e.g.*, Pl. PCOL ¶¶ 56-62; Chernoby Aff. ¶ 67.

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court agrees with the Attorney General's interpretation, then it should further clarify that the term "shall … not require any authorization by the manufacturer" allows the manufacturer to remain in the access loop and does not impede a manufacturer's ability to limit which particular persons can access a vehicles' on-board diagnostic systems and vehicle networks—such that OEMs can implement secure gateways and other tools that restrict such access and authenticate who may access their vehicle systems. Doing so may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular provision/aspect of the Data Access Law. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular statutory requirement or the Data Access Law in general, and compliance would take years to accomplish given other statutory requirements, including the "standardization" language and requirement for administration by a third party.

- Attorney General's position: The term "authorization" means an actor's role or what it is and is not permitted to do on a system. Authorization is distinct from authentication, which refers to the confirmation of the identity of an individual, user, or other actor.

  Contrary to Auto Innovators' argument, the trial evidence established that an "authorization system" which provides "access to vehicle networks and their on-board diagnostics systems," "is standardized across all makes and models sold in the Commonwealth" and is "administered by an entity unaffiliated with a manufacturer," as required by Section 2, can be implemented in a timely manner without increasing cybersecurity risks. *See* AG Rev. FF ¶¶ 172-96. Because Section 2 only requires manufacturer authorization to a

vehicle's on-board diagnostic system to be administered by an unaffiliated entity, it does not limit the ability of a manufacturer to require authentication or impose any requirements on access controls, Mode 27, or other safety techniques that do not require authorization by the manufacturer. *See* AG Rev. FF ¶¶ 13-15, 47-48, 172-96, 211. The trial evidence further established that many OEMs allow access to their on-board diagnostic systems without requiring any manufacturer authorization at all. *See* AG Rev. FF. ¶ 172-74; Tr. II: 108-09, 129, 217-18; Potter Aff. ¶¶ 44-48, 56.

E. "Directly or indirectly"

The parties do not agree on the definition of this term.

- Auto Innovators' position: The term "directly or indirectly" means that the OEM may not impose the requisite authorization either by itself or through some third party.

- Attorney General's position: The term "directly or indirectly" here means that the manufacturer may not require any authorization by the manufacturer itself or a third party controlled by or affiliated with the manufacturer.

F. "An entity unaffiliated with a manufacturer"

The parties agree on the definition of this term, but disagree about OEMs' ability to comply with this definition's requirements.

- Auto Innovators' position: The term "entity unaffiliated with a manufacturer" means an entity that does not have a formal corporate affiliation with an OEM. The law does not specify whether "an entity unaffiliated with a manufacturer" would include an entity that is outside of the manufacturer's corporate control, but within its indirect control, such as through a contract. However, Auto Innovators understands that the proponents of the Data Access Law did not intend to limit this language to apply only to direct corporate affiliates.

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that "an entity unaffiliated with a manufacturer" could be an entity that is within the direct or indirect control of the manufacturer (notwithstanding a lack of formal corporate affiliation or control), then that may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular provision/aspect of the Data Access Law because it may permit OEMs to, for example, contractually impose minimum privacy and cybersecurity standards and controls on the unaffiliated entity(ies) that may be administering the access system. However, no such "entity" currently exists. *See, e.g.*, June 15 Tr. 27:16-18, 97:1-7, 125:6-9. Particularly if the relevant "authorization system" must be "standardized" across all OEMs and administered by a single entity unaffiliated with any manufacturer, it will take years to develop and

implement such an entity, as the entire auto industry will need to agree on the form, structure, and function of such an entity (with input not only from OEMs, but also other industry players and government regulators). *See, e.g.*, Pl. PFOF ¶¶ 134-36 (describing practical difficulties in developing necessary infrastructure, lengthy development of NASTF, and OEMs' continued involvement in authorization process). Further, the use of such a single entity would not eliminate the cybersecurity risks associated with this particular provision, as creating a single entity responsible for authorization may facilitate intrusions into multiple manufacturers' vehicles at once. This would increase cybersecurity attack surface and risk exponentially. *See, e.g.*, Tierney Aff. ¶¶ 93-94.

- Attorney General's position: The term "entity unaffiliated with a manufacturer" means an entity that does not have a formal corporate affiliation with an OEM or is subject to an OEM's direct or indirect control.

  Contrary to Auto Innovators' argument, the trial evidence established that "an entity unaffiliated with a manufacturer" can be created without compromising the security or integrity of vehicle networks or requiring the removal of access controls. *See* AG Rev. FF, ¶¶ 61, 177-79; Tr. Ex. 30 at 3-4; Tr. II:89. The trial evidence established that administration of authorization systems by an unaffiliated entity is common and well-established in other industries, such as internet web browsers. *See* AG Rev. FF. ¶¶ 177-79. The trial evidence further established that such an unaffiliated entity can be readily created, but the OEMs have refused to work with others in the auto industry to put together such an entity. *See* AG Rev. FF. ¶¶ 46-49, 192-96; Lowe Aff. ¶¶ 68-69, 71-74, 82, 88-89; Tr. II:88-89.

III. Interpretation of Terms in Section 3

Section 3 of the Data Access Law provides that:

[c]ommencing in model year 2022 and thereafter a manufacturer of motor vehicles sold in the Commonwealth . . . that utilizes a telematics system shall be required to equip such vehicles with an inter-operable, standardized and open access platform across all of the manufacturer's makes and models. Such platform shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. Such platform shall be directly accessible by the owner of the vehicle through a mobile-based application and, upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by an independent repair facility or class 1 dealer . . . limited to the time to complete the repair or for a period of time agreed to by the vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle. Access shall include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair.

Mass. G.L. c. 93K, § 2(f).

A. "Telematics system"

The parties agree on the definition of this term.

- Auto Innovators' position: The term "telematics system" is defined by statute as "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information . . . utilizing wireless communications to a remote receiving point where it is stored."

  Notwithstanding Auto Innovators understanding of this provision as described above, if the Court determines that the term "stored" refers only to information that is accumulated by the manufacturer or placed in a data collection system for later use by the manufacturer, that may exclude some motor vehicles from the scope of Section 3.

- Attorney General's position: The term "telematics system" means "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information . . . utilizing wireless communications to a remote receiving point where it is stored."

B. "Inter-operable"

The parties agree on the definition of this term, but disagree about what this definition requires and about OEMs' ability to comply with those requirements.

- Auto Innovators' position: The term "interoperable" means a standard way to connect and communicate with the vehicle. An interoperable device is one that can be used regardless of the manufacturer.

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that the term "interoperable" requires inter-operability across all makes and models of a specific OEM, rather than all manufacturers, that may reduce the loss of cybersecurity protections by reducing threat actors' ability to target multiple manufacturers' vehicles through a single attack. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular statutory requirement or the Data Access Law in general. Further, no "inter-operable" platform of the type described in the Data Access Law currently exists, and it will take years to develop and implement such a platform, with an even longer time required for one that is "inter-operable" among all manufacturers.

  In response to the Attorney General's comment below, Auto Innovators further notes that the evidence at trial established that the Attorney General's experts' proposed solutions for compliance with this provision do not currently exist and would take years to develop (PFOF ¶¶ 104, 122-24), and

that there are major deficiencies and practical difficulties to such proposed approaches. *See, e.g.*, June 15 Tr. 125:19-22 ("dongle" solution only limited to data currently available through OBD-II ports); PFOF ¶ 140 (required "dongle" does not currently exist, creates cybersecurity risk, and would require reconfiguration of vehicles); PFOF ¶ 131 (SVI system does not exist and requires lengthy development); June 15 Tr. 200:11-206:3 (describing steps necessary, including agreement on "data dictionary" developed by tool vendors, before SVI solution could be accomplished). Likewise, disabling telematics is simply a workaround to application of section 3 of the Data Access Law—not compliance with that law—and would result in the disabling of key safety features, firmware-over-the-air capabilities, and consumer services. Pl. PFOF ¶¶ 125-29.

- Attorney General's position: The term "interoperable" means a standard way to connect and communicate with the vehicle. An interoperable device is one that can be used regardless of the manufacturer.

  Contrary to Auto Innovators' argument, the trial evidence established that interoperability can be achieved in a reasonable timeframe without compromising cybersecurity. The trial evidence established at least two potential methods which a given OEM might equip its vehicles with an interoperable platform: utilizing a dongle plugged into the J-1962 port as the diagnostic platform, or designing a fully telematic diagnostic platform contained on the vehicle. *See* AG Rev. FF. ¶¶ 208-32. For the first method, utilizing a dongle and the J-1962 port, the trial evidence demonstrated that the J-1962 connector already provides an interoperable physical connection into the vehicle, and the UDS protocol provides an interoperable method for performing diagnostics, such that using a dongle plugged into the J-1962 connector would achieve interoperability by making access to diagnostic, repair, and maintenance information uniform across the auto industry, using the same connector and methods to perform diagnostics, maintenance, and repair. *See* AG Rev. FF. ¶ 209-21; Smith Aff. ¶¶ 123, 128. For the second method, the trial evidence established that while creation of a fully telematic platform will require time to design, test, and validate, the amount of time will vary depending on the specific OEM and model vehicle. *See* AG Rev. FF. ¶¶ 223-32; Smith Aff. ¶ 207; Tr. I:195 (Plaintiff's expert Bryson Bort agreeing that, if an OEM were to devote the time and resources to make any appropriate changes to its vehicles' architectures, that OEM could securely comply with the Data Access Law). The trial evidence showed that preexisting defined diagnostic functions (like those used by GM and FCA) and the preexisting UDS protocol would also hasten the process of creating a fully-telematic platform. *See* AG Rev. FF. ¶ 232; Tr. III:55-56, 57, 68, 79; Smith Aff. ¶¶ 46, 125, 127-28, 146-48, 195.

  Further, both the trial evidence and supplemental evidence on Subaru and Kia's practices established that OEMs may achieve immediate compliance with Section 3 by disabling or not enabling a telematics system in certain of

their Model Year 2022 or newer vehicles, and safely comply with the Data Access Law while developing an interoperable platform. *See* AG Rev. FF ¶¶ 198-207; Joint Stipulation, ECF No. 262, ¶¶ 2-6; Plaintiff Alliance for Automotive Innovation's Responses to Attorney General Maura Healey's Third Set of Interrogatories, ECF No. 263-1, at 8-9.

C. "Standardized"

The parties agree on the definition of this term, but disagree about what this definition requires and about OEMs' ability to comply with those requirements.

- Auto Innovators' position: The term "standardized" means following a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating.

  No "standardized" platform of the type described in the Data Access Law currently exists, and it will take years to develop and implement such a platform, with an even longer time required for one that is "standardized" among all manufacturers.

  In response to the Attorney General's comment below, Auto Innovators further notes that the evidence at trial established that the Attorney General's experts' proposed solutions for providing "standardized" platforms purportedly compliant with this provision do not currently exist and would take years to develop, and that there are major deficiencies and practical difficulties to such proposed approaches. *See supra* § III.B.

- Attorney General's position: The term "standardized" means following a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating.

  Contrary to Auto Innovators' argument, the trial evidence showed that a standardized platform can be developed in a reasonable timeframe. *See* AG Rev. FF. ¶¶ 221, 224, 229-32; Smith Aff. ¶¶ 121, 208-09; Tr.I:195. The trial evidence established that standardized access to a vehicle's on-board diagnostic systems is already provided by the J-1962 connector. *See* AG Rev. FF. ¶¶ 176, 209-212; Potter Aff. ¶ 14; Smith Aff. ¶¶ 123, 128-30. Moreover, the trial evidence demonstrated that Secure Vehicle Interface, or "SVI," exists as one potential standardized method for securely communicating mechanical data that OEMs can implement with either of the two potential hardware platforms (dongle or fully-telematic platform) that would make the platform "standardized" as required in Section 3 of the Data Access Law. *See* AG Rev. FF ¶¶ 233-245; Tr. III:97.

D. "Open access"

The parties do not agree on the definition of this term.

- Auto Innovators' position: "Open access" means that the relevant device or technology—here, the "platform"—can be accessed without restriction. Such access includes the ability to "send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair."

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that the term "open access" does not preclude a manufacturer from imposing authorization (including authentication) restrictions on access to the platform, and that "open access" does not require the ability to write data to the platform, that may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular provision/aspect of the Data Access Law. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular statutory requirement or the Data Access Law in general. Further, no "open access" platform of the type described in the Data Access Law currently exists, and it will take years to develop and implement such a platform.

  In response to the Attorney General's comment below, Auto Innovators further notes that the evidence at trial established that removing manufacturers from the process of authorizing data written to the vehicles, as the "open access" language requires, would compromise cybersecurity and safety and emissions controls. *See generally* Pl. PFOF ¶¶ 141-46.

- Attorney General's position: The term "open access" means having a non-gated way to gain access to the data and capabilities. An open access platform and the mechanical data it communicates with are freely accessible to the owner, without the OEM acting as a gatekeeper.

  Contrary to Auto Innovators' argument, the trial evidence established that an open access platform can still use security measures to ensure the safety and privacy of the consumer. *See* AG Rev. FF. ¶ 69; Smith Aff. ¶ 115-17. The trial evidence established that common methods of securing communication, including authentication, Mode 27, and "seed and key" security, can be used with the open access platform described in Section 3. *See* AG Rev. FF. ¶¶ 13-15, 69, 172-74, 222.

E. "Platform"

The parties agree on the definition of this term.

- Auto Innovators' position: The term "platform" means the vehicle architecture and associated software and features.

- Attorney General's position: The term "platform" means the vehicle architecture and associated software and features.

F. "Securely communicating"

The parties do not agree on the definition of this term.

- Auto Innovators' position: "Securely communicating" means transmitting data privately, without unpermitted viewing of the content of that transmission.

- Attorney General's position: The term "securely communicating" means communication in a way that authenticates the identities of the recipient and the sender, where the communication is not made known to parties other than the recipient and the sender and the integrity of the communication is not compromised.

G. "Mechanical data"

The parties agree that this term is defined by the statute, but interpret that definition differently, and disagree about OEMs' ability to comply with that definition's requirements.

- Auto Innovators' position: The term "mechanical data" is defined as "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle." As the "otherwise related to" language makes clear, "mechanical data" is not limited to diagnosis, maintenance, and repair data, but actually encompasses *any* vehicle data that could have some bearing on diagnosis, maintenance, or repair issues.

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that the term "mechanical data" is limited to data generated by the vehicle solely for the purpose of diagnosis, maintenance, and repair, that may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular provision/aspect of the Data Access Law. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular provision or the Data Access Law in general. Further, even under that alternative definition of "mechanical data," it would take years to develop and implement such a platform.

- Attorney General's position: The term "mechanical data" means "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle."

H. "Directly accessible"

The parties do not agree on the definition of this term.

- Auto Innovators' position: "Directly accessible" means that the user (*e.g.*, the owner or repair shop) can directly connect to the platform without having to go through any intermediary, including the OEM. That direct access includes the ability to "send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair."

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that access does not require the ability to write data to the platform, and the term "directly accessible" does not preclude a manufacturer from imposing authorization (including authentication) restrictions on access to the platform (*e.g.*, because the manufacturer could grant "direct access" after properly authenticating the user), that may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular provision/aspect of the Data Access Law. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular provision or the Data Access Law in general. Further, even under that alternative definition of "directly accessible," it would take years to develop and implement the platform capable of transmitting data in this manner.

  In response to the Attorney General's comment below, Auto Innovators further notes that the evidence at trial established that the "directly accessible" platform required by section 3 does not currently exist, would take years to develop, and would undermine vehicles' cybersecurity. *See generally* Pl. PFOF ¶¶ 122-24, 130-52.

- Attorney General's position: The term "directly accessible" means that the consumer will not need to go through the OEM to perform diagnosis, maintenance, and repairs.

  Contrary to Auto Innovators' argument, the trial evidence established that a "directly accessible" platform as described in Section 3 of the Data Access Law can be developed in a reasonable timeframe without compromising security. *See* AG Rev. FF. ¶¶ 70, 197-245.

I. "Mobile-based application"

The parties do not agree on the definition of this term.

- Auto Innovators' position: An application on a mobile phone.

  Notwithstanding Auto Innovators' understanding of this provision as described above, if the Court determines that a "mobile-based application" is not necessarily an application on a mobile phone but could include an

application built into the vehicle itself (as the Attorney General's expert suggested at trial, *see* June 15 Tr. 207:4-208:7), that may reduce the loss of cybersecurity protections that otherwise would occur through compliance with this particular provision/aspect of the Data Access Law. However, that interpretation of the statute would not eliminate the cybersecurity risks associated with this particular provision or the Data Access Law in general. Further, no such "mobile-based application" currently exists, and it will take years to develop such applications. Pl. PFOF ¶ 123.

- Attorney General's position: An application on a mobile device. A mobile-based application could be implemented as an in-dashboard display in a vehicle, or as part of a software application on a mobile phone that could be offered to accompany a vehicle.

J. "Ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair"

The parties do not agree on the definition of this term.

- Auto Innovators' position: This term refers to the user's ability to write data to any vehicle component when such writing is necessary for maintenance, diagnostic, or repair purposes.

  As the United States observed in its Statement of Interest, "all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence," so "this requirement effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle's systems—including braking, steering, and acceleration." ECF No. 202 at 7. It is precisely this definition that forms one of the bases for Auto Innovators' preemption challenge.

- Attorney General's position: The term "ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair" means the ability to write diagnostic data to vehicle ECUs, and to transmit packets to the ECU, if necessary for the maintenance, diagnosis, or repair of a vehicle.

  Contrary to Auto Innovators' argument, the "ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair" does not require access to write data to any vehicle component. Rather, the trial evidence established that it only requires access to write data to vehicle ECUs, and to transmit packets to the ECU, if necessary for the maintenance, diagnosis, or repair of a vehicle. *See* AG Rev. FF ¶ 73; Tr. Ex. 30 at 7. As established by the expert testimony of Craig Smith, "the ability to send commands to in-vehicle components" can be given in a way that preserves security and enables independent shops and vehicle owners to make necessary repairs. *See* Tr. Ex. 30 at 7; Defendant's Amended Trial Affidavit of Craig Smith, ECF No. 192, ¶ 119, 133-37, 142, 173.

Respectfully submitted,

PLAINTIFF ALLIANCE FOR AUTOMOTIVE INNOVATION,

By its attorneys,

/s/ Laurence A. Schoen

Laurence A. Schoen, BBO # 633002
Elissa Flynn-Poppey, BBO# 647189
Andrew N. Nathanson, BBO#548684
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY, AND POPEO, P.C.
One Financial Center
Boston, MA 02111
Tel: (617) 542-6000
lschoen@mintz.com
eflynn-poppey@mintz.com
annathanson@mintz.com

John Nadolenco (*pro hac vice*)
Erika Z. Jones (*pro hac vice*)
Jason D. Linder (*pro hac vice*)
Daniel D. Queen (*pro hac vice*)
Eric A. White (*pro hac vice*)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
jnadolenco@mayerbrown.com
ejones@mayerbrown.com
jlinder@mayebrown.com
dqueen@mayerbrown.com
eawhite@mayerbrown.com

Charles H. Haake (*pro hac vice*)
Jessica L. Simmons (*pro hac vice*)
ALLIANCE FOR AUTOMOTIVE INNOVATION
1050 K Street, NW
Suite 650
Washington, DC 20001
Tel: (202) 326-5500
chaake@autosinnovate.org
jsimmons@autosinnovate.org

DEFENDANT ATTORNEY GENERAL MAURA HEALEY,

By her attorneys,

/s/ Christine Fimognari

Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Christine Fimognari, BBO No. 703410
Assistant Attorneys General
Office of the Attorney General
One Ashburton Place
Boston, Mass. 02108
(617) 963-2206
Christine.fimognari@mass.gov

CERTIFICATE OF SERVICE

I hereby certify that I served the foregoing document on October 7, 2022, electronically to opposing counsel of record as follows:

Laurence A. Schoen, Esq.
lschoen@mintz.com

Elissa Flynn-Poppey, Esq.
eflynn-poppey@mintz.com

Charles H. Haake
chaake@autosinnovate.org

Jessica L. Simmons
jsimmons@autosinnovate.org

Erika Z. Jones, Esq.
ejones@mayerbrown.com

Eric A. White, Esq.
eawhite@mayerbrown.com

John Nadolenco, Esq.
jnadolenco@mayerbrown.com

/s/ Christine Fimognari
Christine Fimognari
Assistant Attorney General

October 7, 2022