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. _____.

COMPLAINT

Plaintiff Alliance for Automotive Innovation (Auto Innovators) brings this complaint for declaratory and injunctive relief, and alleges as follows:

INTRODUCTION

1. This action challenges Massachusetts SD645 (2019-2020) (the "Data Law"), passed by ballot initiative and now codified at Chapter 93K of the Massachusetts General Laws.

2. The nation's leading car and light truck manufacturers—the members of Auto Innovators—take seriously their role as careful stewards of sensitive vehicle data. Each member recognizes that access to that data, and to the secured vehicle systems that generate that data, could, in the wrong hands, spell disaster. Massachusetts's new Data Law will reduce the security of these systems, seriously hampering manufacturers' attempts to keep vehicle data and vehicle systems safe.

That is not hyperbole. The federal agency charged with promoting vehicle safety has expressed those concerns about this very law.

3. The National Highway Traffic Safety Administration ("NHTSA") provided written testimony to the Massachusetts Legislature's Joint Committee on Consumer Protection and Professional Licensure last July, stating that the ballot initiative would force "vehicle manufacturers to redesign their vehicles in a manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible." NHTSA's letter is attached to this complaint as Exhibit A. NHTSA concluded that, if enacted, the Data Law would "prohibit manufacturers from complying with both existing Federal guidance and cybersecurity hygiene best practices," putting the public at risk by compromising the integrity of such vital vehicle functions as braking, acceleration, and steering. Ex. A Ltr. at 2. NHTSA's concerns were not hypothetical but grounded in real-world experience. As the agency explained to the Joint Committee, NHTSA had recently participated in a recall for one auto manufacturer because of cybersecurity concerns around unprotected vehicle systems that hackers could exploit to compromise vehicle safety. *Id.* at 3. The Data Law poses a substantial threat of amplifying and spreading that cybersecurity risk through all new vehicles sold in Massachusetts.

4. The ballot initiative's proponents falsely touted the measure as necessary to provide Massachusetts consumers with a "right to repair" their vehicles by granting vehicle owners access to vehicle maintenance data necessary to have

repairs performed at their preferred non-dealership maintenance shops. But consumers already enjoy the freedom to have their vehicles repaired at the shops of their choice. And existing law (*i.e.*, prior to the adoption of the Data Law) gives those repair shops—right down to mom-and-pop independents—as well as vehicle owners easy access to any vehicle mechanical data necessary to make those repairs.

5. Pre-existing Massachusetts law—buttressed by industry-led, nationwide commitments—already mandates that auto manufacturers "shall provide access to their onboard diagnostic and repair information system[s]" and that, to the extent any proprietary device were necessary to access the data on those systems, that device be made "available to independent repair facilities upon fair and reasonable terms." Mass. Gen. L. ch. 93K, § 2(d)(1). In short, Massachusetts consumers have had a robust "right to repair" long before the Data Law. There is no evidence that members of Auto Innovators have blocked independent auto repair shops from accessing data necessary to assess vehicle performance and conduct maintenance and repair.

6. Under the guise of providing access to data necessary to perform vehicle maintenance, the Data Law sweeps broadly to allow third-party access to nearly all data generated by vehicles—with negative consequences for consumer privacy, public safety, and manufacturers' federally protected property rights.

7. Big-box auto-parts retailers (and others) have long sought access to more data about their customers and potential customers that they can use to profile individuals and increase sales. For instance, many vehicles generate data to issue

in-vehicle messages that routine maintenance will be needed. A third-party retailer would like access to this data to be able to target consumers for marketing.

8. The Data Law facilitates this data grab, in part, through capacious new definitions that make nearly all vehicle data accessible by third parties. The law defines "Mechanical Vehicle Data" broadly to include "*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." SD645 § 1 (emphasis added). Data "otherwise related to" diagnosis, repair, or maintenance could be interpreted to sweep in most data generated, stored in, or transmitted by a motor vehicle.

9. With respect to "telematics system data" and other "mechanical data," the law imposes extremely broad access requirements. First, it requires that access to vehicle "on-board diagnostic systems" in any vehicles "sold in the Commonwealth" be "standardized and not require the use of any authorization, directly or indirectly, by the manufacturer," unless a standardized authorization system is used across all vehicle makes and models and is administered by a third party. SD645 § 2. No such system currently exists.

10. Second, the law addresses "telematics systems," which it defines as "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such [data] utilizing wireless communications to a remote receiving point where it is stored." SD 645 § 1. The law provides that, for any automaker "that utilizes any telematics system" in its vehicles—which means just

about every automaker—the automaker must, by Model Year 2022 (which automakers can begin selling as early as January 2, 2021), develop and install in all of its vehicles sold in Massachusetts a standardized, open-access, bi-directional "platform" allowing third parties unfettered access to use and alter the "mechanical data emanating from the motor vehicle" to the platform. SD645 § 3. That is, under the law, auto manufacturers must abandon the current secure vehicle systems that they have spent substantial time and money building and maintaining, and instead design, test, and manufacture from whole cloth a new system that allows third parties to retrieve data from, modify data in, and write data to, the vehicle through a "platform" over which the manufacturer would have no control.

11. Failure to comply with these requirements will subject auto manufacturers to substantial fines—amounting to several times the manufacturers' profit margin on a given vehicle, with nearly limitless liability if the same vehicle is taken to multiple repair shops—or even outright exclusion from the Massachusetts vehicle market.

12. Far from protecting consumers, the law puts consumer safety at risk by allowing third parties to access, and modify, that data on auto manufacturers' systems without the manufacturers' authorization. Indeed, the law does not permit auto manufacturers to keep in place measures that are currently installed to secure the integrity of their vehicle systems and the data contained on them. And to compel this open structure, the Data Law expressly mandates that auto manufacturers forgo their right to exclude third parties from using their intellectual property and viewing

their trade secrets. Perhaps most significantly, the Data Law fails to address the negative consequences for consumers and automakers resulting from requiring the installation of an open-access, bi-directional telematics system—something that does not exist today—by the end of this year.

13. The public is harmed, not helped, by this law. The Data Law threatens consumer safety. In June 2020, the Massachusetts Legislature's Joint Committee on Consumer Protection and Professional Licensure asked NHTSA—the federal agency responsible for enforcing vehicle safety and performance standards—to provide written testimony regarding whether and to what extent the Data Law, if enacted and enforced, might pose safety and cybersecurity risks. NHTSA concluded that mandating an open access vehicle platform accessible to third parties—and especially one that allows those third parties to overwrite vehicle data—would "prohibit manufacturers from complying with both existing Federal guidance and cybersecurity hygiene best practices," putting the public at risk by compromising the integrity of such vital vehicle functions as braking, acceleration, and steering. Ex. A Ltr. at 2.

14. NHTSA further testified that, if enacted, the Data Law would require "vehicle manufacturers to redesign their vehicles in a manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible." Ex. A Ltr. at 2. And by doing so, NHTSA stated, the Data Law creates a "direct conflict" with federal law. *Id.* at 4.

15. What is more, Massachusetts's law creates serious data privacy risks, threatening to compromise the integrity of consumers' data and security. Auto manufacturers follow strict industry standards (and, where applicable, federal laws) to maintain the confidentiality of sensitive vehicle data. But if the Data Law is allowed to take effect, years of manufacturers' work and billions of dollars in investment to protect and secure vehicle data will effectively be obliterated. As a result, Massachusetts citizens run the risk of having their personal and confidential information (such as their telephone call records or places they visit) exposed to third parties who may not have the same stringent obligations to protect consumer data that auto manufacturers observe, and who may not be sufficiently capable of protecting that data. That data could easily find its way into the hands of bad actors who could track and monitor consumers or target public officials—exposing highly sensitive personal information or ransoming that information to keep it from being exposed. And the lack of system controls that this law would bring would facilitate the ability of nefarious actors to hack into consumers' vehicles by way of "telematics" access, creating potentially substantial risks to consumer privacy. The cost of such a data breach to any individual auto manufacturer would be devastating—injuring consumers, potentially subjecting manufacturers to liability, and putting at risk the manufacturer's hard-earned reputation for safe vehicle performance in the highly competitive auto market. Put simply, if a hacker breaches a given manufacturer's vehicle system as a result of the Data Law's requirement to create unprotected systems, *that* manufacturer—not the Commonwealth or the big-box auto-parts chains

that championed the law and stand to benefit from it—will get the blame, be subject to liability, and have their reputations and brand images tarnished.

* * *

16. As documented in NHTSA's letter, Massachusetts's Data Law violates federal law. It is preempted under the Supremacy Clause of the U.S. Constitution because it conflicts with federal law and policy regarding a host of consumer safety and intellectual property protections. It also takes auto manufacturers' private property without providing just compensation in violation of the Fifth Amendment as incorporated by the Due Process Clause of the Fourteenth Amendment.

BACKGROUND

17. Auto Innovators is the leading advocacy group for the auto industry. It was formed in 2020 from the combination of the country's two largest industry trade associations, the Alliance of Automobile Manufacturers and the Association of Global Automakers, to provide a single, unified voice for the auto industry. Auto Innovators' members are the country's leading auto manufacturers. Together, the group's members produce nearly 99 percent of the cars and light trucks sold in the United States today. Vehicles manufactured by those members are sold throughout the country, including in Massachusetts, both through dealership sales and aftermarket used sales.

18. Modern vehicles have changed a great deal since the advent of the automobile. Vehicles sold in the United States today are often as much marvels of technology as they are of mechanics. At tremendous expense, Auto Innovators' members have developed electronic systems for the vehicles in their production

lineup to provide the functionality of the vehicles they sell in the increasingly high-tech new automobile market demanded by consumers.

19. But high-tech automobiles necessarily present cybersecurity challenges. As the FBI observed in a 2019 report, as a result of increasing Internet-connectivity the "automotive industry will face a wide range of cyber threats and malicious activity in the near future," with vehicles "a highly valued target for nation-state and financially motivated actors." Josh Campbell, CNN, *FBI Says Hackers Are Targeting US Auto Industry* (Nov. 20, 2019), https://www.cnn.com/2019/11/20/politics/fbi-us-auto-industry-hackers/index.html. To address this threat Auto Innovators' members have made substantial investments to design and put in place access controls that guard the security and performance of vehicle systems. The controls limit access to the secure parts of those systems (and the data they protect) to those authorized by the manufacturer, in accordance with the manufacturer's regulatory obligations to its customers as well as its property rights and licensing agreements.

20. The Data Law would upend the careful balance struck among three goals: maintaining tight access controls to sensitive vehicle data; protecting manufacturers' intellectual property rights; and allowing consumers and the repair shops of their choice access to any data necessary for vehicle diagnosis, repair, or maintenance. In place of that balance, the Data Law charts a course into the unknown—requiring auto manufacturers such as Auto Innovators' members to abandon their existing, secure vehicle systems and develop entirely new, "open access" systems that allow third parties to pull, push, and rewrite vehicle data (and

in some cases, push software updates) at will, which could affect the actual functionality and safety of the vehicle.

21. Because the Data Law will become effective December 3, 2020, *see* Mass. Const. Amends. Art. 48, Pt. V, § 1, Auto Innovators' members face imminent risk of enforcement of the law against them—with penalties ranging all the way up to exclusion from the automobile market. As discussed below, some of the law's requirements take effect right away - including removing manufacturers' control over access to vehicle on-board diagnostic systems (SD645 § 2) and the law's onerous penalty provisions (*id.* § 2). Other portions of the law (*id.* § 3) go into effect beginning model year 2022 ("MY2022")—which, given industry lead times, is materially no different than right away, because MY2022 sales can begin as early as January 2, 2021. The extraordinary changes required by the law, combined with the standard industry lead time necessary to develop future model year vehicles, means that most members will be incurring substantial costs immediately in an attempt to comply with the law. And if an automaker cannot research, develop, and implement the open-access, bi-directional platform required by the Data Law for its MY2022 vehicles, then it could be subject to significant penalties for its vehicles sold in Massachusetts, whether directly through dealers or in the aftermarket.

22. The new statutory obligations that will be imposed upon Auto Innovators' members regarding third-party open access to proprietary vehicle systems and confidential data pose a real and immediate threat to consumer data privacy and safety and to manufacturers' property rights.

THE PARTIES

23. Plaintiff Alliance for Automotive Innovation (Auto Innovators) is a nonprofit trade association with its corporate headquarters and principal place of business in Washington, D.C. Its members include BMW of North America, LLC; FCA US, LLC; Ford Motor Co.; General Motors Co.; Honda North America, Inc.; Hyundai Motor America; Jaguar-Land Rover North America, LLC; Kia Motors America, Inc.; Mazda North America; Mercedes-Benz USA, LLC; Mitsubishi Motors of North America, Inc.; Nissan North America, Inc.; Porsche Cars North America, Inc.; Subaru of America, Inc.; Toyota Motor North America, Inc.; Volkswagen Group of America; Volvo Cars USA.

24. Defendant is the Attorney General of the Commonwealth of Massachusetts. In that position, she is the State's chief law enforcement officer and is responsible for enforcing the Data Law. The Attorney General is sued in her official capacity only.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over Auto Innovators' claims pursuant to 28 U.S.C. §§ 1331, and 2201(a). There is federal question jurisdiction under 28 U.S.C. § 1331 because Auto Innovators alleges violations of the federal Constitution and federal law. Auto Innovators, on behalf of its members, seeks a declaration of its rights pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, over which there is an actual controversy after the enactment of the Data Law.

26. This Court has personal jurisdiction over Defendant because (a) she is located in the District in which this action was filed; and (b) many of the actions giving rise to these claims occurred in and/or were directed from this District.

27. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b) and (c).

FACTUAL ALLEGATIONS

A. Auto Manufacturers' Electronic Vehicle Systems and Access Controls

28. Auto Innovators' members developed and maintain, own, and operate proprietary vehicle systems that generate "mechanical data" as defined in the Data Law. Much of this information is not needed to assist in the diagnosis, repair, or maintenance of vehicles—and, to the extent it is needed for diagnosis, repair or maintenance, the information is already available to repair shops. The systems developed by the Auto Innovators' members contain software that is used to transmit or access data that is separate and apart from data utilized to assist in the diagnosis and repair of vehicles. These systems operate through proprietary source code displayed in the software used to access and modify vehicle data. And they are maintained through firmware updates that also use member-developed code.

29. Auto Innovators' members have made substantial investments to build and support their network of vehicle system products and software. Collectively, they have spent billions of dollars researching, developing, and deploying new and enhanced system products for their customers.

30. Many members of Auto Innovators grant limited personal licenses to purchasers of their vehicles to access and use various components of vehicle systems. Auto repair shops and consumers currently have varying levels of data access, which

depend on obtaining consent and agreeing to use that access only for authorized purposes. For a number of reasons—most critically, safety—no consumer (or third party) has access to every component of a vehicle's systems.

31. Under current law, independent repair facilities have access through the on-board diagnostic port to all on-board vehicle information necessary for diagnosis, maintenance, and repair of that vehicle. But only individuals and entities expressly authorized by Auto Innovators' members may access other data in the vehicle that are not necessary for diagnosis, maintenance, and repair. This includes Controller Area Network (CAN) bus messages that communicate among a vehicle's electronic control units to allow the vehicle to perform core vehicle functions like acceleration, steering, and braking. This type of prior authorization ensures the safety and security of the vehicle and its systems, and permits "contact tracing" of who had access to the CAN bus in the event that the system malfunctions after the repair was performed.

32. Because of the importance of secure vehicle systems to vehicle safety, Auto Innovators' members do not allow anyone—customer, dealer, or third party—unrestricted access to those systems beyond what is necessary for diagnosis, maintenance, and repair without a valid license or the member's express permission. Unauthorized access and modification of vehicle data at will could create significant safety concerns, resulting in untold amounts of liability risk for auto manufacturers.

33. By maintaining strict controls over access to vehicle systems, Auto Innovators' members are able to ensure that unauthorized third parties do not have

the ability to obtain or, more ominously, rewrite software at the electronic control unit level—which, as NHTSA recognizes, could seriously impair the safety and functionality of vehicles.

33. Protecting the integrity and security of vehicle systems and the data they generate is of paramount concern to each of Auto Innovators' members. To that end, members employ a variety of technologically advanced security features to protect their systems, related components, installed firmware, and the data compilations stored on the systems—all to guard against unauthorized access that could compromise members' intellectual property rights, vehicle safety, vehicle security, and customer privacy. These access and security controls include, for instance, encryption keys, unique IDs, password protections, asymmetric keys exchanged between vehicle systems and a member's servers, authorized message requirements, secure boot, secure storage, network domain segregations, and firewalls designed to control (and protect) the flow of messages in vehicle systems.

34. Auto Innovators' members are continuously researching, developing, and implementing new security measures to protect against unauthorized users circumventing access controls and accessing their vehicle systems. Many members have dedicated teams employed by them or by an affiliate who protect and defend members' systems from cybersecurity threats. These measures depend on the automaker having control over the relevant information access points—something the Data Law would prohibit.

35. All told, the measures taken by Auto Innovators' members help to effectively maintain access control by ensuring access to their intellectual property is reserved only to those with their express permission or in accordance with their licensing agreements.

36. The development and implementation of these access and security controls are necessary to keep hackers and other unauthorized parties out of vehicle systems and to ensure the safe operation of members' vehicles in accordance with industry standards and federal law.

B. The Massachusetts Data Law

37. As explained above, Auto Innovators' members have developed systems that enable authorized users to access members' vehicle data in managed, secure, and reliable ways when that access is justified and done in accordance with members' property rights and licensing agreements.

38. Massachusetts's Data Law eviscerates the substantial investments that Auto Innovators' members have made in those systems and requires members to expend untold more time and money creating new platforms that risk compromising the security and functionality of members' systems and vehicles.

39. Broadly speaking, the Data Law contains two requirements. First, it requires that access to vehicle on-board diagnostic systems via port-hookup be "standardized and not require the use of any authorization, directly or indirectly, by the manufacturer," unless a standardized authorization system is used across all vehicle makes and models and is administered by a third party. SD645 § 2. This mandate must be satisfied immediately. In addition, the law addresses vehicles with

a "telematics system," which it defines 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." *Id.*. The law requires manufacturers to equip any vehicle sold in Massachusetts that uses a "telematics system" with "an inter-operable, standardized and open access platform across all . . . makes and models" "[c]ommencing in model year 2022." SD645 § 3. That platform must be "directly accessible" by the vehicle owner through an (undefined) "mobile-based application" as well as by independent repair facilities, and must allow these parties "to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair." *Id.* And the platform must be "capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform"—*i.e.*, without auto manufacturers having any control over it. *Id.*

40. The law ties these requirements to an expansive definition of the data covered by these two requirements. Specifically, the law defines "mechanical data" broadly to include all 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." SD645 § 1 (emphasis added). There is no obvious limit to the reach of the law, particularly given the law's broad applicability to any vehicle with a "telematics system." *Id.* § 3.

41. Even though part of the law is pegged to MY2022, all of its effects will be felt immediately. The law requires Auto Innovators' members to create and

implement its first-of-its-kind "open access" system on a grossly unrealistic timeframe. Many members have already completed the development of their MY2022 lineups—unsurprising given that vehicles from that model year can be sold as early as January 2, 2021.

42. The Data Law's timeframe presents serious practical problems that will impact cybersecurity and vehicle safety. Most of Auto Innovators' members do not currently provide standardized, wirelessly accessible on-board diagnostics systems (which they now must do immediately) or "open access" systems (which they now must do by MY2022—*i.e.*, also immediately) across their entire vehicle lineup. For instance, the systems available on a base-model truck may be technologically quite distinct from those on a car loaded with options including a navigation package. The lead time to create entirely new systems is close to five years, and then many years after that to accomplish a standardized system across all models in a lineup. Such a system would first have to be designed, developed, and tested, followed by a period of safety-impact assessments for any changes that implicate core vehicle functions, and only then could a manufacturer *begin* to roll out a new system on *some* of its models. The Data Law therefore sets an impossible task. It defies reality in the auto industry to think that MY2022—mere weeks away—is in the distant future or in any way provides sufficient lead time to comply with the Data Law's requirements.

43. The Data Law thus leaves each automaker with an impossible choice. It may seek to avoid running afoul of at least some of the Data Law, for instance, by no longer selling "in the Commonwealth" a vehicle "that utilizes a telematics system."

SD645 § 3. That approach would deprive any manufacturers' would-be customers of significant benefits afforded by modern vehicle technology. Alternatively, an automaker could elect to continue selling such vehicles in the Commonwealth, by attempting to comply (in vain) with the requirements of the Data Law by abandoning existing access controls, trying to cobble together some sort of "open access" platform across all of its makes and models, and granting wide-ranging, on-demand licenses to access that platform so that third parties may use and alter data on its vehicles' systems. Either way presents immediate significant risks for consumers and substantial costs to manufacturers.

44. To make matters worse, these radical changes—on a compressed, unrealistic timeline—are not necessary to allow car-buyers to choose to have their vehicles serviced at the facility of their choice. Consumers across the country have been able to do that for decades. Since 2013, Massachusetts law has confirmed that right by requiring that consumers and independent auto repair shops have access to information needed to diagnose, repair, and maintain vehicles. Mass. Gen. L. ch. 93K. That law reflected a balance between ensuring consumer and independent auto repair shop access while still protecting consumer data protection and safety as well as manufacturers' intellectual property.

45. The Data Law upends that balance by opening up vehicles manufactured by Auto Innovators' to widespread unauthorized (and uncontrolled) third-party access.

46. Manufacturers must equip any MY2022 vehicle sold in Massachusetts that uses a "telematics system" with "an inter-operable, standardized and open access platform across all . . . makes and models." SD645 § 3. The Data Law thus requires Auto Innovators' members to abandon their proprietary vehicle systems, design and build entirely new systems that lack necessary security controls over confidential vehicle data on a highly expedited timeframe, and allow all comers to access those systems regardless of members' intellectual property rights:

47. And the Data Law requires Auto Innovators' members to abandon their intellectual property rights to exclude unauthorized users from their systems. Under the law, the new platform must be accessible by the vehicle owner and by independent repair facilities and must allow these parties "to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair." SD645 § 3.

48. By defining "access" capaciously to "include the ability to send commands to in-vehicle components if needed for the purpose of maintenance, diagnostics and repair," SD645, § 3, it requires Auto Innovators' members not just to permit unauthorized third parties to pull data from their systems but also to change existing data or software, or insert new data or software into their systems.

49. In its purpose and effect, then, the Data Law grants broad third-party access to vehicle systems and data and does not provide a framework sufficient to safeguard those systems and data.

50. The open-access platform required by the Data Law is significantly less secure than the current systems Auto Innovators' members have invested substantial resources building, which require users to obtain authorization from the applicable manufacturer before gaining access.

51. Open access violates the fundamental security tenet known as data-minimization-or-least-privilege access, which—consistent with federal laws and industry standards—holds that each user of a secured system should receive no greater access or privileges than necessary. That principle is embodied in the current approach taken by Auto Innovators' members, which ensures that authorized users access only the specific categories of data needed for that user's specific legitimate purpose.

52. This problem is not remedied by the Data Law's "authorization" requirement. Any system that contemplates a wider distribution of access, particularly with read/write privileges, necessarily increases the risk of cybersecurity breach and misuse. Moreover, even if the "authorization" requirement worked perfectly in practice, it would not stop owners themselves from making modifications to vehicle systems—*e.g.*, an owner could potentially disable emissions controls to increase vehicle performance, in contravention of federal environmental and safety standards—nor does it ensure that the shop owner's systems are hardened against potential unauthorized access to a vehicle's systems.

53. The Data Law includes extremely harsh penalties for non-compliance. For one, it expressly permits vehicle owners and independent repair shops to sue auto

manufacturers like Auto Innovators' members for violations of the statute and recover treble damages or a minimum penalty of $10,000 per event. SD645 § 4.

54. But the law also contemplates subjecting violators to "any remedy authorized by chapter 93A" of the Massachusetts General Laws. *Id.*; *see also* Mass. Gen. L. ch. 93K, § 6 ("In addition to any other remedies that may be available, a violation of this chapter shall be deemed to be an unfair method of competition and an unfair or deceptive act or practice in the conduct of trade or commerce in violation of section 2 of chapter 93A."). Section 2 of Chapter 93A provides the Attorney General with the power to craft regulations and remedies for what are deemed "unfair" or "deceptive" acts. *See* Mass. Gen. L. ch. 93A, § 2(c). The Attorney General can, for instance, seek injunctions against violators. *See id.* § 4. And "habitual" violators of those injunctions risk being shut out of the Massachusetts market altogether. *Id.* § 8 ("Upon petition by the attorney general, the court may for habitual violation of injunctions . . . order the dissolution, or suspension or forfeiture of franchise of any corporation or the right of any individual or foreign corporation to do business in the commonwealth.").

55. Moreover, the law does not on its face limit liability to sales by new vehicle dealers in Massachusetts. Manufacturers could thus face these substantial penalties if *any party* were to sell a vehicle in Massachusetts, including a used vehicle, that does not comply with the Data Law's onerous new requirements.

C. The Data Law Compromises Vehicle and Data Security

56. As discussed above, the Data Law upends members' extraordinary investments in vehicle-system access and security controls by explicitly banning the

use of such controls by mandating what it terms an "open access" system with the ability to read, modify, and write third-party data at will.

57. Auto Innovators' members have good reasons for maintaining tight control over access to their vehicle systems. Vital vehicle components are controlled by vehicle systems affected by the Massachusetts law. As NHTSA explained, these systems play a role in such core vehicle functions as steering, braking, and acceleration. Access controls for vehicle systems are necessary to prevent compromising the safe performance of these vehicle functions. A hacker could, for instance, cause the vehicle to accelerate without application of the accelerator pedal, or prevent the brakes from working when the vehicle exceeds a certain speed. A sophisticated hacker could even install software with delayed activation, such as disabling the brake system one month after repair is performed—making it virtually impossible to identify the malevolent actor or hold him accountable for the harm. Whatever form they take, the consequences of such an event due to compromised or non-existent access controls could be disastrous. Threats to cybersecurity are an ever-present danger today—and require constant vigilance from manufacturers to stave off. The Data Law makes the ability to perform, and to scale, such threats far easier than ever before.

58. In particular, many of Auto Innovators' members are concerned that being forced to eliminate access controls to provide the Data Law's contemplated "open access" system may compromise the secure gateways between data stored onboard (that may include such things as location or driver performance) and a

vehicle's CAN bus. The CAN bus is the vehicle's information superhighway; it is at the center of all vehicle functions. A third party with nefarious intent could cause significant harm if it were to gain control over a vehicle's CAN bus and, thus, critical vehicle functions. The breadth of the Data Law's requirements—and the aggressive timeframe in which they would take effect—might require disabling CAN bus message filters and other means used to segregate system components at the time vehicles were designed. This could render many existing cybersecurity controls around the CAN bus effectively nonfunctional. At the very least, the Data Law's required "open access" platform could provide an exploitable portal into a vehicle's CAN bus, allowing a malevolent actor the ability to tamper with the software governing the operation of safety-critical vehicle systems, like the braking system.

59. Moreover, vehicle systems may generate or store sensitive consumer information. To take just one example, data may include detailed vehicle geolocation information. The same data that allow a vehicle navigation system to be able to accurately locate vehicles in the event of an accident could, in the wrong hands, provide incredibly detailed information about the vehicle owner's driving habits. Studies have shown that it only takes four randomly selected time and space coordinates to identify a person with 95% accuracy. *E.g.*, Y.A. de Montjoye et al., Unique in the Crowd: The Privacy Bounds of Human Mobility. Sci. Rep 3, 1376 (2013). https://doi.org/10.1038/srep01376. Geolocation data "provides an intimate window into a person's life, revealing not only his movements, but through them his familial,

political, professional, religious, and sexual associations." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (internal quotations omitted).

60. Auto Innovators' members expend considerable effort to maintain the confidentiality of any sensitive consumer information generated by vehicle systems. For years, those members have followed industry guidelines set out in their shared Consumer Privacy Protection Principles—which sets a minimum floor for data protections that members are free to exceed. At the core of these principles is the minimization and de-identification of data, as well as a commitment to employ reasonable measures to protect against the unauthorized access or use of data.

61. Moreover, Auto Innovators' members have controls in place to protect consumer data not only because that reflects best practices in the automotive industry, but also because federal law in many contexts requires them to do so. Numerous federal laws and regulations limit how consumer data may be handled, stored, or processed.

62. For example, for well over a decade, the Federal Trade Commission has recommended that companies "[l]imit[] access to customer information to employees who have a business reason to see it," and to ensure that only properly authorized individuals are able to access a system. FTC, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (Apr. 2006); *see* 8 CFR § 314.4 (Safeguards Rule). The FTC has taken action against companies that fail to take sufficient steps to protect consumer data from hackers under data-protection laws like the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), and others. And because they

routinely finance customers' purchase or lease of new vehicles, several of Auto Innovators' members are considered to be like financial institutions that regulators contend are subject to applicable regulations.

63. Under the regime contemplated by the Data Law, auto manufacturers will not be able to require a third-party accessing a vehicle system to meet the same or similar security measures that the auto manufacturer requires of itself, affiliates, and service providers.

D. Federal Regulators Recognize the Inherent Safety Problems in the Data Law

64. There is considerable danger to consumers from an open access platform, particularly one with the ability to send commands—*i.e.*, to write data to the system. The government agency charged with promoting uniform federal safety standards, NHTSA, warned the Massachusetts Legislature of precisely this danger while the Data Law was under consideration.

65. In written testimony provided at the request of the Joint Committee considering the Data Law, NHTSA explained that the Data Law's provisions compromise federal regulations promoting vehicle safety. *See* Ex. A Ltr.

66. NHTSA concluded that "two of the most important techniques" to promote consumer safety—"logical and physical isolation of vehicle control systems from external connections, and controlling access to firmware that executes vehicle functions"—are rendered "impossible" by the Data Law. Ex. A Ltr. at 4-5.

67. NHTSA observed that the Data Law "requires vehicle manufacturers to redesign their vehicles in a manner than necessarily introduces cybersecurity risks,

and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible." Ex. A Ltr. at 5.

68. NHTSA concluded that the Data Law would "create a direct conflict with existing Federal guidance." Ex. A Ltr. at 4. Where NHTSA recommends isolating logical and physical control systems, the Data Law "requires" precisely the opposite. *Id.*

69. NHTSA labeled as a "key" part of its federal vehicle-safety guidance the principle "that manufacturers should control access to firmware that executes vehicle functions." Ex. A Ltr. at 3. NHTSA added that this control "is particularly important for firmware controlling vehicle motion such as steering, acceleration, and braking," *id.*—all features closely tied to vehicle safety that are extensively regulated by NHTSA.

70. NHTSA also identified the impracticability of what the Data Law requires manufacturers to accomplish in a short period of time. For instance, NHTSA addressed the novelty of the unified system architecture contemplated by Massachusetts's law, noting that it was "not aware of any existing system architectures that would satisfy the requirements" of the Data Law. Ex. A Ltr. at 3. Based on its considerable expertise in the automotive industry, NHTSA informed the Massachusetts Legislature that such a system was "unlikely to be developed, tested, validated and deployed in the proposed timeframe" contemplated by the law. *Id.*

71. As a result, NHTSA said, the Data Law in effect "would require [manufacturers] to remove all access controls from their telematics systems,

including controls designed to ensure the security of safety-critical systems" in order to comply with the law. Ex. A Ltr. at 3. And doing so, NHTSA concluded, would "raise substantial safety risks for American families." *Id.*

72. In the end, NHTSA was clear that the Data Law would frustrate federal safety standards: "The ballot initiative would require manufacturers to provide remote functionality that may potentially pose an unreasonable risk to safety, and further, eliminate their flexibility and ability to provide appropriate remote access controls." Ex. A Ltr. at 4.

73. NHTSA's concern about the impact of technological access vulnerabilities occasioned by the Data Law on federal safety standards is grounded in real-world experience. In 2015, NHTSA found several of Chrysler's vehicles to have a flaw in their radio software security that "could allow unauthorized third-party access to some networked vehicle control systems." FCA, Safety Recall R40 / NHTSA 15V-461, Radio Security Vulnerability 2 (July 2015), https://static.nhtsa.gov/odi/rcl/2015/RCRIT-15V461-7681.pdf. There, NHTSA determined that third-party "[e]xploitation of the software security vulnerabilities could lead to exposing the driver, the vehicle occupants or any other individual or vehicle with proximity to the affected vehicle to a potential risk of injury." *Id.* Ultimately, Chrysler worked with NHTSA to conduct—at great expense—a voluntary recall of 1,410,000 vehicles to repair the software vulnerability. *Id.*

74. In its letter to the Joint Committee, NHTSA observed that the Data Law could lead to the same (or worse) problem that it had to address in the Chrysler recall.

See Ex. A Ltr. at 3 n.6. After all, the law mandates authorized users of the system be able "to send commands to in-vehicle components if needed for the purposes of maintenance, diagnostics and repair." SD645 § 3. That would allow a hacker not only to be able to read private information, but also to send commands to vehicles, potential causing harm as serious as stopping vehicles in the road or disabling vehicles' braking systems. *See* Ex. A Ltr. at 3.

75. In short, as NHTSA's findings indicate, the Data Law creates an imminent risk to driver and passenger safety.

E. Federal Law Protects Manufacturers' Intellectual Property

76. As discussed above, the Data Law *mandates* that manufacturers create, install, and maintain an "open access" system in their fleets sold in Massachusetts, limited only by the insufficient and easily circumvented requirement that the vehicle owner grant permission. That means that third parties, without members' authorization, would be able to access members' systems, download data, and even *change* data or *add* new data to those systems at will.

77. In doing so, the Data Law would disrupt the investment-backed expectations of Auto Innovators' members. Those members have invested billions of dollars to develop the hardware and software components of vehicle systems over recent years. Under existing law, members are able to recoup some of their ongoing financial investment in vehicle systems and the data they organize—through, for example, licensing arrangements with affiliates (for software to access vehicle systems) or consumer subscription plans (for certain types of services, like

navigation). The Data Law interferes substantially with those reasonable, investment-backed expectations.

78. The vehicle systems of Auto Innovators' members are suffused with valuable intellectual property. Many members have proprietary firmware (*i.e.*, software programmed onto a hardware device that allows the device to operate as intended, such as by allowing systems to control various vehicle components) in their systems, including any diagnostics sub-components. And many members make vehicle systems accessible through proprietary software, wirelessly and by direct connection, that they have developed and routinely update. Other proprietary member software allows individual system components to communicate with each other or allow individual computers or software components to communicate with each other. And some members have developed proprietary methods of organizing the vehicle systems data themselves, which transform otherwise indecipherable raw data into usable data compilations.

79. The systems included in members' vehicles are original and independent works created, operated, and maintained by members or their affiliates. These systems—including their various components, including but not limited to installed firmware, hardware, software, and unique methods of compiling data—consist of original and distinct elements. Among their original and creative elements are their source and object code; distinctive screen layouts; graphical content; text arrangement, organization, and display of information; and dynamic user experience.

80. In addition to their core functionalities, vehicle systems process and store voluminous amounts of sensitive consumer data, including, where applicable, those related to system performance, navigation, diagnostics, and vehicle function.

81. Auto Innovators' members have spent considerable time and money developing these systems and determining the types of information to include (and exclude) in those systems. Members are continually engaged in design and development to refine the function and safe operation of vehicle systems and maintain secure connections between vehicle data and members' servers.

82. It is virtually impossible for a third-party user to access or use vehicle systems without running Auto Innovators members' copyrighted firmware, software, and unique method for compiling data, at least without (intentionally or unintentionally) introducing significant safety issues. In many cases, the act of running these components copies proprietary elements of those systems to the user's computer. Moreover, unless properly authenticated through manufacturer-controlled mechanisms, a user who writes additional data to the systems necessarily interferes with the integrity of the system and the data stored on it.

83. Members' property interests in their vehicle systems are protected by federal law. Several statutes protect members' rights to exclude in a way that is flatly contradicted by the "open access" and read/write regime mandated by the Data Law.

84. The Copyright Act provides that "[a]nyone who violates any of the exclusive rights of the copyright owner . . . is an infringer of the copyright or right of the author." 17 U.S.C. § 501(a). The Act enables any "legal or beneficial owner of an

exclusive right under a copyright . . . to institute an action for any infringement of that particular right committed while he or she is the owner of it." 17 U.S.C. § 501(b).

85. The Digital Millennium Copyright Act ("DMCA") provides that no "person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A).

86. As discussed above, Auto Innovators' members employ a variety of access controls to protect their copyrighted works. Attempts by any third party to bypass, avoid, disable, deactivate, or impair these access-control measures by accessing or providing access to unlicensed third parties violates § 1201(a)(1)(A)'s prohibition on circumvention of a technological measure that effectively controls access to a work protected by the Copyright Act and DMCA.

87. Members' vehicle systems are original, creative works subject to copyright protection. Any unlicensed use of those systems (or use exceeding the terms of the license between members, their affiliates, and end users) infringes those copyrights.

88. Auto Innovators' members frequently register their innovations for copyright protection. Some members have, for instance, registered copyrights for several components of their vehicle systems. But whether registered or not, those systems are suffused with original, creative works and are copyright protected. Any unlicensed use of those systems and firmware—or use exceeding the terms of licenses between members and affiliates and end users—necessarily infringes those copyrights.

89. Attempts by any third party to bypass, avoid, disable, deactivate, circumvent, or impair Auto Innovator members' access-control measures by accessing or providing vehicle-systems access to unlicensed third parties violate § 1201(a)(1)(A)'s prohibition on circumvention of a technological measure that effectively controls access to a work protected by the Copyright Act and DMCA.

90. The Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836, *et seq.*, protects owners of trade secrets from misappropriation by third parties. Under the DTSA, owners of trade secrets have a federally guaranteed right to exclude others from obtaining or using their trade secrets. And under that law, permission to use or access a trade secret must be given by the owner of that intellectual property.

91. Several of members' trade secrets essential to members' competitiveness in the automotive market risk being compromised by the Data Law, including proprietary unlock keys, digital watermarks in software used to access and alter vehicle data, algorithms, vehicle updates, security features, and the format and methods of communicating commands between and to vehicle systems. The Computer Fraud and Abuse Act ("CFAA") provides that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," is subject to both criminal and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages and injunctive relief). This statute also provides a private cause of action for "compensatory damages and injunctive relief or other equitable

relief" to anyone who suffers at least $5,000 in damage or loss in any one-year period "by reason of a violation" of its terms. *Id.* § 1030(g); *see id.* § 1030(c)(4)(A)(i)(I).

92. The operation of vehicle systems involves the use of "computer[s]" within the meaning of the CFAA, which defines that term broadly to include not only computing devices as commonly understood but also "any data storage facility or communications facility directly related to or operating in conjunction with such device." *Id.* § 1030(e)(1). The systems are also "protected computer[s]" within the statute's meaning because they are used in and affect interstate and foreign commerce and communications. *See id.* § 1030(e)(2)(B). For many of Auto Innovators' members, the maintenance of vehicle systems as well as the act of remotely pulling data from (and writing data to) those systems necessarily requires the use of computers at manufacturers' offices.

93. Under the CFAA, authorization required for lawful access to a computer system must come from the system's owners, not from its users. Any access to a computer system without (or exceeding) the computer system owner's authorization violates the statute.

FIRST CLAIM FOR RELIEF

Declaratory Judgment

(Conflict Preemption, National Traffic and Motor Vehicle Safety Act, Federal Motor Vehicle Safety Standards)

94. Paragraphs 1–93 above are incorporated herein by reference.

95. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is

unenforceable because it is preempted by the National Traffic and Motor Vehicle Safety Act ("Motor Vehicle Safety Act"), 49 U.S.C. § 30101, *et seq*.

96. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

97. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

98. Over a half century ago, Congress passed the Motor Vehicle Safety Act to protect consumer safety given the increasing number of automobiles on the road.

99. Under the authority of the Motor Vehicle Safety Act, 49 U.S.C. § 30101, *et seq*., the Secretary of Transportation, acting through NHTSA, acts to safeguard the public through education, research, safety standards and enforcement.

100. In furtherance of its congressional objective, NHTSA has adopted several dozen Federal Motor Vehicle Safety Standards ("FMVSS") designed to maintain a nationally uniform set of safety requirements for new motor vehicles. Courts routinely recognize the preemptive effect of NHTSA standards.

101. The Data Law conflicts with several of the FMVSS that NHTSA has promulgated. As NHTSA observed in its written testimony provided at the request of the Joint Committee considering the Data Law, "the initiative would specifically require that telematics platforms be directly accessible through a mobile-based

application, and that this access must include the ability to send commands to in-vehicle components (including, e.g., braking, acceleration, and steering controls)." Ex. A Ltr. at 2. By doing so, the Data Law is in "direct conflict" with federal regulations and NHTSA guidance. *Id.* at 4.

102. NHTSA regulates extensively in the area of braking, acceleration, and steering controls. NHTSA has, for instance, issued several FMVSS regulations designed to "insure safe braking performance under normal and emergency conditions." 49 C.F.R. § 571.105 (hydraulic and electric brake systems); *id.* § 571.121 (air brake system); *id.* § 571.135 (light-vehicle brake systems). Similarly, NHTSA regulates vehicles' ability to control acceleration. *See, e.g.*, *id.* § 571.124 (accelerator control systems). In light of the substantial role technology plays in all new vehicles, the integrity of these vehicle features will necessarily be impacted by the Data Law's mandate for open vehicle system access, adverse to NHTSA regulations. *See* Ex. A Ltr. at 2-4.

103. NHTSA has also directly addressed vehicle electronic systems. For several years, the agency has recognized the importance of limiting authorization to on-board vehicle computers and data to ensure consumer safety. One way NHTSA addresses this concern is through industry guidance. *See Cybersecurity Best Practices for Modern Vehicles* (issued in October 2016). But NHTSA also promulgates formal safety standards in this burgeoning area of concern, in accordance with its broad mandate under the Motor Vehicle Safety Act. This standard recognizes that vehicles increasingly depend on sophisticated technology to control essential functions. *See,*

e.g., 49 C.F.R. § 571.126 (mandating minimum safety standards for electronic stability control systems in lightweight passenger vehicles, which controls among other things vehicle steering, braking, and speed by computer means).

104. Moreover, NHTSA retains broad, congressionally delegated supervisory authority over auto manufacturers to recall vehicles for safety defects. The Motor Vehicle Safety Act gives NHTSA the authority to enforce its provisions by requiring manufacturers to recall vehicles that fail to meet a vehicle safety standard, or that have a safety-related defect. *See* 49 U.S.C. §§ 30118-120. As part of this supervisory authority to promote vehicle safety, NHTSA develops guidance like the cybersecurity best practices guide discussed above, to address safety problems proactively before recalls are necessary.

105. As NHTSA has recognized, and as discussed above, the Data Law frustrates and is inconsistent with the regulatory framework it has developed under the FMVSS.

106. Moreover, the Data Law also conflicts directly with the Motor Vehicle Safety Act. The Motor Vehicle Safety Act provides that a "manufacturer . . . may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard prescribed under this chapter unless the manufacturer . . . reasonably believes the vehicle or equipment will not be used (except for testing or a similar purpose during maintenance or repair) when the device or element is inoperative." 49 U.S.C. § 30122. Auto Innovators' members have installed

components to comply with various FMVSSs (*e.g.*, air bags, braking systems, steering systems, accelerator controls), nearly all of which are now controlled electronically, and for which members have installed safeguards to prevent electronic intrusion as part of their designs. By mandating an "open access" security regime over vehicle systems that generate data, the Data Law requires auto manufacturers to "make inoperative" safeguards built into the design of these important components, in conflict with Federal law.

SECOND CLAIM FOR RELIEF

Declaratory Judgment

(Conflict Preemption, Clean Air Act)

107. Paragraphs 1–106 above are incorporated herein by reference.

108. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is unenforceable because it is preempted by the Clean Air Act, 42 U.S.C. § 7401, *et seq*.

109. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

110. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

111. The Clean Air Act authorizes the Environmental Protection Agency ("EPA") to establish National Ambient Air Quality Standards ("NAAQS"). EPA

routinely issues regulations to promote a uniform nationwide system of emissions standards. *E.g.*, 40 C.F.R. Part 86 (light-duty motor vehicles).

112. The Clean Air Act effectively nationalizes the standards for emission control devices in new motor vehicles, preventing a patchwork of state regulation. The law itself provides that no state "shall adopt or attempt to enforce any standard relating to the control of emissions" subject to the EPA's Clean Air Act authority. 42 U.S.C. § 7543(a).

113. The Data Law conflicts directly with the Clean Air Act. The Clean Air Act provides that it is prohibited "for any person to remove or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter prior to its sale and delivery to the ultimate purchaser." 42 U.S.C. § 7522(a)(3)(A). In this way, the Clean Air Act seeks to prevent anyone from allowing vehicles' emissions control systems to be circumvented.

114. Emissions-control defeat devices often operate through the use of aftermarket software uploaded to vehicle systems. For instance, a vehicle owner or manufacturer with access to a vehicle's engine control module could disable emissions control systems through the use of software designed for that purpose. This disabling software could have the effect of dramatically increasing engine power at the cost of reducing or eliminating the effectiveness of required vehicle emissions controls.

115. Auto Innovators' members have installed components to comply with stringent EPA emissions control regulations, much of which are now controlled

electronically, and for which members have installed safeguards to prevent electronic intrusion as part of their designs. By mandating an "open access" security regime over vehicle systems that generate data, the Data Law requires auto manufacturers to "render inoperative" these safeguards built into the design of these important components, in conflict with Federal law.

THIRD CLAIM FOR RELIEF

Declaratory Judgment

(Conflict Preemption, Copyright Act)

116. Paragraphs 1–115 above are incorporated herein by reference.

117. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is unenforceable because it is preempted by the federal Copyright Act.

118. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

119. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

120. The Copyright Act, 17 U.S.C. § 101, *et seq.*, offers protection to creators of copyrightable material, including the right to exclude others from copying, distributing, preparing derivative works based on, and displaying copyrighted works.

121. As explained, members' vehicle systems contain copyrighted and copyrightable material. The components of those systems—including but not limited to the firmware associated with them, their hardware, the software used to access them, and the unique methods of compiling data contained on them—are original creative works protected under Title 17. Among their original and creative elements are their source and object code; distinctive screen layouts; graphical content; text arrangement, organization, and display of information; and dynamic user experience. Moreover, the manner in which members compile vehicle data on their systems means that the organization of that data qualifies as creative work protected under Title 17.

122. The Data Law conflicts with, and is preempted by, the federal Copyright Act because it eliminates the copyright owner's right to exclude others from copying, distributing, creating derivative works based on, or displaying the copyrights or copyrightable material by requiring the owner to allow third parties with no authorization from Auto Innovators' members to access and use those members' copyrighted systems, firmware, software, and related components.

123. Such access and use necessarily entails the display, distribution, and creation of copies and derivative works of the copyrighted systems and components.

124. As explained above, often, when a user accesses a vehicle's system to read or write data, that process creates a new fixed copy of the original computer program code in the computer's random access memory.

125. Moreover, allowing third parties to remotely access (and to modify) vehicle systems necessarily entails the distribution of new copies of system firmware, software, and code.

126. Indeed, by allowing third parties to modify the code in vehicle systems without a manufacturer's authorization, the Data Law encourages the unauthorized creation of derivative works in members' systems.

127. State law deprives Auto Innovators' members of their rights under the Copyright Act by requiring them to disseminate works in violation of the Act's protections, and the Data Law stands as an obstacle to the purposes of the Copyright Act.

128. Thus, the Data Law conflicts with the Copyright Act and is preempted.

FOURTH CLAIM FOR RELIEF

Declaratory Judgment

(Conflict Preemption, Defend Trade Secrets Act)

129. Paragraphs 1–128 above are incorporated herein by reference.

130. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is unenforceable because it is preempted by the federal Defend Trade Secrets Act ("DTSA").

131. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

132. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

133. The DTSA, 18 U.S.C. § 1836, *et seq.*, protects owners of trade secrets from misappropriation by third parties. Congress intended the DTSA to be a powerful tool to protect trade secrets: The Act not only establishes criminal penalties, but also gives the owner of a trade secret that is misappropriated a private right of action against anyone who discloses or uses that secret without the owner's consent despite knowing or having reason to know that knowledge of the trade secret was derived from or through someone who had a duty to maintain the owner's secret.

134. In enacting the DTSA, Congress sought to give trade secret owners the right to exclude others from their trade secrets, by providing a federal civil remedy for misappropriation of trade secrets. The Data Law forces Auto Innovators' members to disseminate the very trade secrets that Congress sought to protect, and thus directly conflicts with Congress's goals.

135. Members' vehicle systems—including but not limited to firmware, hardware, software, and the unique compilation of data contained on those systems—comprise and contain many proprietary trade secrets. These trade secrets include proprietary unlock keys, digital watermarks in software used to access and alter vehicle data, algorithms, vehicle updates, security features, and the format and methods of communicating commands between and to vehicle systems. Maintaining

these proprietary trade secrets is vital to members' competitiveness in the auto market.

136. Members' trade secrets relate to the integrity of their vehicle systems and the sound functioning of their vehicles, and are often licensed and/or sold in interstate and foreign commerce. As described in greater detail above, Auto Innovators' members have taken reasonable measures to maintain control over access to their individual systems and thus preserve the secrecy of their trade secrets embodied in those systems.

137. The Data Law conflicts with, and is preempted by, the DTSA because it deprives Auto Innovators' members of their federally protected right to exclude others from their trade secrets by requiring them to provide access to their vehicle systems to third parties without members' authorization.

138. Although Massachusetts law regarding auto repair generally provides that "[n]othing in this chapter shall be construed to require a manufacturer to divulge a trade secret," Mass. Gen. Laws ch. 93K, § 3, the Data Law can be read to do just that—requires divulging trade secrets—by mandating open access to the proprietary vehicle systems of Auto Innovators' members without allowing members to deny authorization or else contracting with a third party to provide a uniform system for access across all vehicle platforms.

FIFTH CLAIM FOR RELIEF

Declaratory Judgment

(Conflict Preemption, Computer Fraud and Abuse Act)

139. Paragraphs 1–138 above are incorporated herein by reference.

140. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is unenforceable because it is preempted by the federal Computer Fraud and Abuse Act ("CFAA").

141. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

142. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

143. The CFAA provides that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," is subject to criminal and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages and injunctive relief).

144. Congress intended the CFAA to empower businesses and individuals to control who may access their computer systems by prohibiting hackers and others from accessing computers without the owners' authorization. Under the statute, computer owners have exclusive discretion to decide who is authorized to access their computer and for what purposes. The CFAA is not only enforceable criminally, but also permits any private person "who suffers damages or loss by reason of a violation

of" the statute to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

145. Members' vehicle systems, the components that communicate via telematics, are "computer[s]" within the meaning of the CFAA. The statute defines that term to include "any data storage facility or communications facility directly related to or operating in conjunction with [a computing] device." 18 U.S.C. § 1030(e)(1). And the vehicle systems to which the Data Law requires "open access" rely on the operation of one or more computing devices owned by members, given the required use of computers by some members to update vehicle systems and to communicate with other computers when data is read or modified. Members' systems for recording vehicle data—and the computing devices by which this data is stored, wirelessly accessed, and altered—constitute "protected computers" within the statute's meaning because they are connected to the Internet and thus are used in and affect interstate and foreign commerce and communications. *See id.* § 1030(e)(2)(B).

146. Contrary to Congress's purpose in enacting the CFAA, the Data Law would eliminate the right of Auto Innovators' members to determine who is an authorized user or for what purpose third parties may use their vehicle systems, by requiring members to construct an open-access platform for accessing a broad array of vehicle data.

147. Thus, the Data Law conflicts with statutory rights federally protected by the CFAA and is preempted.

SIXTH CLAIM FOR RELIEF

Declaratory Judgment

(Conflict Preemption, Digital Millennium Copyright Act)

148. Paragraphs 1–147 above are incorporated herein by reference.

149. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is unenforceable because it is preempted by the Digital Millennium Copyright Act ("DMCA").

150. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land."

151. State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

152. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

153. Congress enacted the DMCA, 17 U.S.C. § 1201, to reinforce copyright owners' rights to use technological defenses to control access to and prevent the copying of copyrighted material. The DMCA establishes penalties for those who circumvent copyright owners' technological defenses. Section 1201(a)(1)(A) of the DMCA provides that no "person shall circumvent a technological measure that effectively controls access to a work protected under this title." Section 1201(a)(2)

reinforces that prohibition by banning commerce in products and services intended to facilitate circumvention of access controls.

154. And the DMCA provides copyright owners with a private right of action against those who unlawfully access an owner's work, *id.* § 1203.

155. Members' vehicle systems—including but not limited to their individual components, the firmware associated with them, their hardware, the software used to access them, and the unique methods of compiling data contained on them—are original creative works protected under Title 17. Among their original and creative elements are their source and object code; distinctive screen layouts; graphical content; text arrangement, organization, and display of information; and dynamic user experience.

156. Moreover, the manner in which members compile vehicle data on their systems means that the organization of that data qualifies as creative work protected under Title 17.

157. Members employ several technological measures to control access to and prevent copying of their vehicle systems and related components and data organizations. These technological measures include a diverse array of encryption, password-protection, and secured messaging, as discussed above. Though each members' particular methods are different, each effectively controls access to critical parts of members' vehicle systems, components, and data. Moreover, each cannot—beyond the bounds of members' licensing agreements and without members' express

authorization—be accessed or run, and their original, expressive elements cannot be displayed or copied unless these access control measures have been navigated.

158. The DMCA prohibits third parties from circumventing these technological measures without the copyright owner's authorization. And the DMCA prohibits third parties from offering services that facilitate circumvention of the above-described technological measures. The DMCA gives Auto Innovators' members enforceable rights against third parties' unauthorized access to and copying of their respective copyrighted systems, components, and data compilations.

159. The Data Law stands as an obstacle to the purposes behind, and is preempted by, the DMCA because it effectively compels Auto Innovators' members to abandon the technological measures that they have adopted to control access to their copyrighted works and that Congress has authorized them to employ. Contrary to the DMCA, the Data Law requires copyright owners like Auto Innovators' members to jettison technological measures and grant open access to their copyrighted systems, components, and the data compilations contained therein without license or authorization from the copyright owner.

SEVENTH CLAIM FOR RELIEF

Declaratory Judgment

(Unconstitutional Taking, U.S. Constitution)

160. Paragraphs 1–159 above are incorporated herein by reference.

161. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that the Data Law is

unenforceable because it works an unconstitutional taking under the U.S. Constitution.

162. The Takings Clause of the Constitution provides that private property may not be taken for public use without just compensation. U.S. Const. amend. V. The Takings Clause is incorporated as to the States through the Due Process Clause of the Fourteenth Amendment. *Chicago, Burlington & Quincy R.R. Co. v. City of Chicago*, 166 U.S. 226, 234-35 (1897).

163. The Data Law deprives Auto Innovators' members of their substantial intellectual property rights. The Data Law accomplishes both a regulatory and physical taking without just compensation.

164. On its face, the Data Law compels Auto Innovators' members to abandon access controls around its on-board diagnostic systems by December 3, 2020, SD645 § 2, and to develop entirely new, "open access" platforms to allow unauthorized third parties to read, modify, and write new data to manufacturers' vehicle systems in time for the 2022 model year, *id.* § 3. Each requirement thus accomplishes a regulatory taking by legislatively restricting members' control over access to their proprietary systems and requiring that access be given to third parties.

165. In practice, the Data Law also physically takes members' private property by requiring them to allow third parties to access and use their existing proprietary systems to remove and write data (and/or new code) to those systems. The law also requires members to provide necessary software to third parties, without members' authorization, to access and modify members' systems at will. The Data

Law thus accomplishes a physical taking by authorizing third parties to physically occupy and take part of members' proprietary systems. In effect, those without members' authorization are granted a permanent easement over members' property.

166. The law upsets the reasonable investment-backed expectations of Auto Innovators' members. Because of the new Data Law, members will unexpectedly be forced to give vehicle owners and independent repair shops open access through a new platform to scores of vehicle data unnecessary to vehicle maintenance and repair. And the character of the government action also demonstrates the presence of a taking, because members are forced to license vehicle systems access that they control to any and all third parties.

167. The Data Law takes private property for no public purpose but rather for the sole economic benefit of a small number of private parties—ostensibly, independent auto-repair shops but in reality big-box chains in the lucrative tools-and-parts business and, eventually, third-party data syndicators. The law provides no corresponding benefit to Auto Innovators' members. In short, the law requires automakers to immediately surrender their valuable intellectual property free of charge.

168. Auto Innovators' members spent significant time and money developing their vehicle systems—collectively, billions of dollars—including security measures to control access to those systems. During that time the government did not regulate the right of dealers to grant third parties access to data unnecessary to vehicle maintenance and repair. Indeed, Massachusetts law was careful to exclude open

access to vehicle systems—including telematics systems, as understood in the industry—in previous legislative efforts.

169. The new Data Law provides no compensation for the physical and regulatory taking of the property of Auto Innovators' members.

170. The new Data law reduces the economic value of vehicle systems to Auto Innovators' members by requiring extensive (and costly) modification of existing vehicle systems, the creation of new "open access" systems, the use of unsecured systems that could compromise safe vehicle function and lead to expensive recalls and damage to members' reputations, and the deprivation of members' rights to exclude others from—and recoup investments in—their vehicle systems.

EIGHTH CLAIM FOR RELIEF

Preliminary and Permanent Injunction

171. Paragraphs 1–170 above are incorporated herein by reference.

172. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority.

173. Auto Innovators has a substantial likelihood of success on the merits of its claims.

174. Auto Innovators' members would suffer irreparable harm in the absence of a preliminary and permanent injunction because the open access to members' vehicle systems required by the Data Law will compromise the integrity of those systems and the safe operation of consumer vehicles, place protected consumer data at risk, and run the risk of permanently and immeasurably damaging members' reputations in the auto industry.

175. As discussed above, the Data Law requires Auto Innovators' members to allow third parties to write data and/or software through their vehicle systems, regardless of whether those parties have been vetted by the members. This dramatic change to existing practices poses the real possibility of data corruption and compromises to vehicle and passenger safety as understood under federal law. Additionally, Auto Innovators' members have expended considerable resources to take strong measures to prevent hackers and other unauthorized users from accessing their systems and data; the methods they have employed are undone by the Data Law, which strips members of their ability to prevent unauthorized access. All the while, confidential information and safe, legitimate vehicle system performance is needlessly placed at risk by the law. And this at a time when the FBI (among others) recognizes that automobiles are a sought-after target for cybersecurity hacking attempts. *See, e.g.*, Chris Chin, *US Automakers Were Leading Targets for Hackers in 2018: FBI*, The Drive (Nov. 21, 2019), https://www.thedrive.com/tech/31150/fbi-claims-us-automakers-were-leading-targets-for-malicious-hackers-in-2018-report (discussing recent FBI report discussing cybersecurity risks in the auto industry, access-control recall, and an experiment by software developers who were "able to commandeer the electric steering and brake control of a Jeep Cherokee at the time by wirelessly hacking into the car's main computer through an [on-board diagnostic II] connector").

176. Auto Innovators' members face untold amounts of harm from complying with the Data Law's open-access requirements—including harm to their business

reputations, exposure to claims by customers, and the considerable costs of conducting recalls mandated by NHTSA to address the predictable results of safety vulnerabilities occasioned by the Massachusetts Law.

177. And those members will be incurring substantial costs immediately, in an attempt to comply with the Data Law's onerous requirements that take effect on an unrealistic timeframe. Further, if Auto Innovators members are required to comply with the Data Law now and the Data Law is later held unconstitutional, it will be impossible to "put the toothpaste back in the tube," and Auto Innovators members' rights will be permanently and irreparably compromised.

178. For these reasons, there is no adequate remedy at law to compensate for the irreparable harm Auto Innovators' members would face if the Data Law is not enjoined during the pendency of this action.

179. The balance of the equities weighs in favor of granting an injunction. Defendant and third parties will not be harmed by the injunction, which would preserve the status quo, in which Massachusetts consumers enjoy complete diagnostic data access (to the extent any such data is necessary for vehicle diagnosis, repair, and maintenance) to have their vehicles repaired at any facility they choose or to enable the repair themselves. Conversely, Auto Innovators' members face irreparable harm to their vehicle systems and professional reputation, members and their customers face exposure of confidential information, and the public face significant safety risks through the novel open-access vehicle-system structure required by the Data Law.

180. The public interest would be served by granting an injunction. The public has a strong interest in halting the enforcement of unconstitutional laws. As NHTSA recognized, the Data Law directly conflicts with federal law. Even aside from the conflict, the public interest is served by protecting consumer safety and data security. Allowing the Data Law to take effect would seriously compromise those public interests, with no corresponding public benefit.

PRAYER FOR RELIEF

Plaintiff respectfully requests that the Court enter judgment:

A. Declaring that the Data Law is unenforceable because it is preempted by the Motor Vehicle Safety Act and Federal Motor Vehicle Safety Standards;

B. Declaring that the Data Law is unenforceable because it is preempted by the Clean Air Act;

C. Declaring that the Data Law is unenforceable because it is preempted by the Copyright Act;

D. Declaring that the Data Law is unenforceable because it is preempted by the Defend Trade Secrets Act;

E. Declaring that the Data Law is unenforceable because it is preempted by the Computer Fraud and Abuse Act;

F. Declaring that the Data Law is unenforceable because it is preempted by the Digital Millennium Copyright Act;

G. Declaring that the Data Law is unenforceable because it violates the Takings Clause of the U.S. Constitution;

H. Temporarily and permanently enjoining the enforcement of the Data Law;

I. Awarding Plaintiff its costs and litigation expenses, including attorneys' fees and costs;

J. Awarding Plaintiff such other and further relief as the Court deems just, proper, and equitable.

Dated: November 20, 2020

Respectfully submitted,

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

Andrew J. Pincus (*pro hac vice* pending)
Erika Z. Jones (*pro hac vice* pending)
Archis A. Parasharami (*pro hac vice* pending)
Eric A. White (*pro hac vice* pending)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
apincus@mayerbrown.com
ejones@mayerbrown.com
aparasharami@mayerbrown.com

eawhite@mayerbrown.com

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