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 **PUBLIC REDACTED VERSION** **Leave to File Excess Pages Granted June 22, 2021**

PLAINTIFF'S PRE-ARGUMENT BRIEF

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Federal Constitutional Provisions and Statutes

State Constitutional Provisions and Statutes

Other Authority

INTRODUCTION

The evidence at trial demonstrated that the Data Access Law imposes impossible requirements on original equipment manufacturers ("OEMs")—ones that, were OEMs to attempt to comply, would unconstitutionally frustrate and conflict with federal law. Section 2 of that law requires OEMs to deploy a non-existent standardized system for accessing vehicle data, and it contemplates a non-existent third-party entity to control access to that data. Section 3 of that law requires OEMs to equip their vehicles with an inter-operable, standardized, open access platform that does not exist, with that platform directly accessible through a mobile-based application that also does not exist. And yet both sections require near-immediate compliance—with Section 2 taking effect just one month after voter approval and applicable to all vehicles model year 2018 and newer, *see* Mass. Const. amends. art. 48, pt. V, § 1, and Section 3 set to take effect with the imminent sale of model year 2022 vehicles, *see* Data Access Law § 3 (codified at Mass. Gen. Laws ch. 93K, § 2(f) (2020))—with enforcement of the two provisions stayed only by this litigation.

The trade association that crafted the terms of the Data Access Law, and pushed that law at the ballot box, knew all along that none of the essential elements of the law's requirements existed. *See* June 15 Tr. at 13:5-22 (Lowe). But, to them, that was an intentional feature, not a bug. *See* Ex 62 (at 38567-68); June 15 Tr. at 50:25-53:3 (Lowe) (discussing Ex. 62). They deliberately imposed requirements they knew could not be met, with impossible timeframes for compliance, in hopes that by doing so they would gain not just mean advantage, but the "ultimate bargaining chip" over OEMs. Ex. 62 (at 38568); June 15 Tr. at 52:25-53:1 (Lowe).[1]

[1] The Auto Care Association ("ACA") sold the Data Access Law to Massachusetts voters as a way to take control of vehicle data, but in reality it was about them getting access to that data, not for repair (they already had all the data they needed for that) but for marketing purposes. *See, e.g.*, Exs. 62, 68. That explains the millions of dollars that the auto parts aftermarket and the trade groups representing them poured into the ballot effort, June 15 Tr. at 20:16-21:6 (Lowe), with an extra $185,000 to the Attorney General's Office to help defend against this lawsuit, *see id.* at 58:4-7 (Lowe). And it was about other business opportunities, too—like monetizing the new regime contemplated by the Data Access Law, by charging Massachusetts drivers an annual fee for cybersecurity, *see id.* at 53:10-54:2; *see also*

All of that was supposed to be at some point in the distant future. *See* June 15 Tr. at 52:7-9 (discussing 2025 as the planned completion date). Meanwhile, OEMs do not have the luxury of waiting for a third-party entity to get up to the task of securely managing access to all vehicle systems in Massachusetts, or for someone to fashion a standardized cyber-secure telematically equipped dongle with access to any and all data a vehicle generates.[2] OEMs are required to comply with the Data Access Law now—at the pain of substantial penalties. *See* Data Access Law § 5.

The unrebutted testimony of Plaintiff's fact witnesses established that the only way OEMs could attempt to comply with the Data Access Law's requirements in the timeframe provided in that law would be to remove the cybersecurity controls they designed and installed in their vehicles to protect safety-and emissions-critical vehicle functions in compliance with applicable Federal Motor Vehicle Safety Standards ("FMVSSs") and emissions regulations. Tierney Aff. ¶¶ 13, 82-106; Baltes Aff. ¶¶ 29-31, 34; Chernoby Aff. ¶¶ 61-62, 65-69, 72, 75, 79, 81-82, 85. The Attorney General's various ideas to speed up the process of compliance—all of which are theoretical and many of which are at odds with the Data Access Law that she defends—do not change that fact. Anything is possible with enough time and resources. But safe and emissions-secure compliance with the requirements in the Data Access Law is entirely theoretical, and at best years away. In the meantime, the Data Access Law "requires 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." Dkt. 202, Statement of Interest of the United States ("U.S. Statement") Ex. 1 at 5.

Ex. 62 (at 38568); Ex. 68 (at 39688-98), without, of course, telling voters that a vote for Question 1 meant having to pay for cybersecurity, *see* June 15 Tr. at 54:3-4 (Lowe).

[2] As the United States points out, "[b]ecause all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, [the Data Access Law] effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle's systems—including braking, steering, and acceleration." U.S. Statement at 7.

ARGUMENT

I. Federal Preemption Principles Demonstrate that the Data Access Law Is Preempted.

The Constitution makes federal law paramount. *See, e.g.*, *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372 (2000) (citing U.S. Const. art. VI, cl. 2). When federal and state obligations conflict, the former controls. *Id.* Conflict preemption comes in two forms—"where it is impossible for a private party to comply with both state and federal requirements, or where state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Freightliner Corp. v. Myrick*, 514 U.S. 280, 287 (1995).

Courts analyze preemption "under the circumstances of th[e] particular case." *Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 873 (2000) (internal quotations omitted). And this is not a case where federal requirements "operate parallel to, rather than in place of" state requirements. *Capron v. Office of Atty. Gen. of Mass.*, 944 F.3d 9, 30 (1st Cir. 2019).

Rather, the federal government is charged by the National Traffic and Motor Vehicle Safety Act ("Safety Act") with preventing "unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle[.]" 49 U.S.C. § 30102(a)(9); *see* U.S. Statement at 2 (describing this as "foundational" to the Safety Act). The Safety Act, in turn, imposes direct obligations on OEMs to help bring this about—by requiring them to certify compliance with FMVSSs, 49 U.S.C. § 30115, and by requiring them to conduct a recall for a defect related to motor vehicle safety, *id.* at §§ 30111, 30116, 30118; *see* U.S. Statement at 2. OEMs are also under a statutory obligation not to make inoperative the design elements they have installed in vehicles to protect regulated functions. *Id.* at § 30122(b). Similarly, the Clean Air Act likewise obligates OEMs to meet stringent emissions standards, 42 U.S.C. §§ 7521(d), 7541(a)(1), and prevents them from rendering inoperative design elements installed to protect emission

systems, *id.* at § 7522(a)(3)(A).

Auto Innovators acknowledges that it bears the burden of proving preemption. *E.g.*, *Capron*, 944 F.3d at 21. But courts consider preemption claims premised on the Safety Act under "ordinary pre-emption principles," without imposing any "special burden" on plaintiffs. *Geier*, 529 U.S. at 870 (rejecting dissent's call for a presumption against preemption). And courts likewise apply "ordinary pre-emption principles" to Clean Air Act preemption claims. *In re Volkswagen "Clean Diesel" Mktg, Sales Prac., & Prods. Liab. Litig.*, 959 F.3d 1201, 1213 (9th Cir. 2020).

Nor is there some heightened threshold because Auto Innovators brought this preemption claim before the Data Access Law took effect. *Cf.* U.S. Statement at 5-6 ("[The] purpose of the Safety Act . . . is to prevent serious injuries stemming from established defects before they occur") (internal quotations and citation omitted). The Attorney General's frequent attempts[3] to make Auto Innovators prove that "no set of circumstances exist" where the Data Access Law could be validly applied is inapt. *See, e.g.*, *Capron*, 944 F.3d at 20 (holding that preemption plaintiffs, even though bringing a facial challenge, "need not show that 'no set of circumstances exists' under which the challenged laws would be valid in any application," but rather only that the "challenged state laws are invalid *as applied* to [the plaintiff's federal requirements]) (emphasis added).[4]

II. OEMs Cannot Comply with the Data Access Law on the Law's Timeframe.

Auto Innovators and its OEM members first learned at trial that even the Attorney

[3] *See, e.g.*, Dkt. 172, Def.'s Trial Memorandum ("AG Tr. Memo."), at 3-5; Dkt. 174 Def.'s Substitute Concls. of Law ("AG CoL"), at ¶ 30.

[4] Indeed, "the particular label of the claim—facial versus as applied—'is not what matters[.]'" *Capron*, 944 F.3d at 20 (quoting *John Doe No 1 v. Reed*, 561 U.S. 186, 194 (2010)). The line between facial and as-applied challenges is often blurry. *Elgin v. Dep't of Treasury*, 567 U.S. 1, 15 (2012); *see also Citizens United v. FEC*, 558 U.S. 310, 331 (2010) ("[T]he distinction between facial and as-applied challenges is not so well defined that it has some automatic effect or that it must always control the pleadings and disposition in every case involving a constitutional challenge."). To the extent the distinction is relevant, it often turns on whether scope of any relief "reach[es] beyond the particular circumstances of the[] plaintiffs." *John Doe No. 1*, 561 U.S. at 194. Here, the reach of any relief would be coterminous with Auto Innovators' membership—obligations imposed on OEMs.

General's own witnesses all agree that OEMs cannot comply with the Data Access Law now or when it passed. That creates a due process problem for OEMs and for the Court—for OEMs because they face stiff penalties for violating a law with which they cannot comply, and for the Court because it cannot construe the law so that compliance with it is possible. A law that commands someone to perform an impossible act is unconstitutional. *See, e.g.*, *United States v. Dexter*, 165 F.3d 1120, 1125 (7th Cir. 1999) (observing that "the validity of a law with which it is impossible to comply may be questioned" as violating the Due Process Clause) (quotations omitted). And this Court has broad equitable power to fashion a just remedy. *See, e.g.*, *Brown v. Plata*, 563 U.S. 493, 538(2011) ("Once invoked, the scope of a district court's equitable powers . . . is broad, for breadth and flexibility are inherent in equitable remedies.").

In an attempt to meet the Data Access Law's requirements, OEMs would have to try to achieve the impossible by removing cybersecurity protections that protect safety- and emissions-critical functions.[5]

A. Section 2 Requires Immediate, Significant Changes.

Section 2 modifies Massachusetts's existing Right to Repair Law. *See* Data Access Law § 2 (codified at Mass. Gen. Laws ch. 93K, § 2(d)(1) (2020)). That 2013 Right to Repair Law already ensures that "independent repair facilities" have access to data necessary to vehicle diagnosis, repair, or maintenance on "fair and reasonable terms." *E.g.*, *See* Mass. Gen. L. ch. 93L, § 2(d)(1) ("Beginning in model year 2018 . . . [e]ach manufacturer shall provide access to the same

[5] To be clear, the inability to comply with the Data Access Law's requirements does not in any way preclude a finding of conflict preemption. *See, e.g.*, *Geier*, 529 U.S. at 882 ("[T]his Court's pre-emption cases do not ordinarily turn on such compliance-related considerations as whether a private party in practice would ignore state legal obligations . . . or how likely it is that state law actually would be enforced. Rather, this Court's pre-emption cases ordinarily assume compliance with the state-law duty in question."); *Ariz. Dream Act Coal. v. Brewer*, 757 F.3d 1053, 1063 (9th Cir. 2014) ("State law is preempted whenever its application would frustrate the objectives and purposes of Congress, even if the state law's own application is frustrated by individuals' noncompliance.").

onboard diagnostic and repair information available to their dealers, including technical updates to such onboard systems, through [] non-proprietary interfaces as referenced in [the law].").[6]

Section 2 of the Data Access Law adds to the existing Right to Repair Law two new alternative requirements: Beginning with model year 2018 vehicles, OEMs must "standardize[]" access to their on-board diagnostic ("OBD") systems and make them accessible "without authorization by the manufacturer, directly or indirectly." Data Access Law § 2. Or they must design and implement an "authorization system for access to vehicle networks and their on-board diagnostic systems" that is "standardized across all makes and models sold in the Commonwealth and . . . administered by an entity unaffiliated with a manufacturer." *Id.* The requirements were scheduled to take effect for model year 2018 vehicles and newer in December 2020, *see* Mass. Const. amends. art. 48, pt. V, § 1; Data Access Law § 2, at pain of fines, enforcement actions, and private suits, *see id.* at § 5.

1. OEMs Cannot Comply with Section 2 Immediately.

It is undisputed that there is no "authorization system for access to vehicle networks and their on-board diagnostic systems" that is "standardized across all makes and models sold in the Commonwealth," Data Access Law § 2. *See, e.g.*, June 15 Tr. 24:24-25-15 (Lowe); *id.* at 96:18-97:3 (Potter).[7] It is likewise undisputed that there is no "entity unaffiliated with a manufacturer" that could run a standardized authorization system, Data Access Law § 2. *See, e.g.*, June 15 Tr. at

[6] That access is further buttressed by a memorandum of understanding ("MOU") that effectively nationalized the requirements in the 2013 Right to Repair Law. *See* Ex. 1 (§ 6); Douglas Aff. ¶ 12. The MOU established a dispute resolution system for access to diagnostic, repair, and maintenance data; in the seven years that the MOU has been in place, no one has ever had to sue over data access or even see a dispute resolution through to completion. *See* June 15 Tr. at 60:18-25 (Lowe).

[7] Complying with the standardization requirement is made all the more difficult given the lack of any attempt in the law to provide a standard. This stands in sharp contrast to the detailed standards provided in the 2013 Right to Repair Law. *See* Mass. Gen. L. ch. 93K, § 2(d)(1) (discussing SAE J2534, SAE J1939, and ISO 22900); *see also* June 15 Tr. at 94:5-95:11 (Potter) (stating that he was surprised that requirements as complex as the Data Access Law's were not given more clarity than a four-page bill).

118:11-13 (Smith); *id.* at 96:18-25 (Potter); *id.* at 13:13-15 (Lowe) ("All along you knew that the third-party entity that is referenced in section 2 does not exist today?" // "Yes.").[8]

That leaves only the first prong of Section 2—which itself requires both standardization of access to OBD systems and access without direct or indirect authorization by the manufacturer. Data Access Law § 2. There is currently no standardized system of access to OBD systems. *See, e.g.*, June 15 Tr. at 25:9-26:7 (Lowe). Although the original Right to Repair Law standardized access through the OBD port itself, OEMs can (and do) require another level of authorization. *See id.* at 24:14-18 (Lowe).[9]

OEMs would thus have to completely upend their secure data access practices, opening the gates to their OBD systems and inviting all comers. *See, e.g.*, June 15 Tr. at 26:13-17 (Lowe) ("[U]nder section 2, Mr. Lowe, either the manufacturer does not require any authorization at all or, if it does, the access has to be standardized and administered by a third party, right?" // "Correct."). The effect would be disastrous. Without a manufacturer (or the unaffiliated third party that does not yet exist) to control authorization, anyone with access to a vehicle and sufficient technical know-how could write compromising data to the vehicle. Bort Aff. ¶ 90. Tellingly, one of the Attorney General's experts expressly declined to opine on the first prong of Section 2. *See* June 15 Tr. at 185:23-186:8 (Romansky). And the other eventually agreed that immediate

[8] *See also* U.S. Statement at 8 "[T]he United States is not aware of any such third party that currently exists, or one that could likely be offered, operationalized, and scaled up to meet the Data Access Law's requirements in the necessary timeframe." Mr. Romansky mentioned AutoAuth as a possible third party, but admitted that he did not know the relationship between FCA and AutoAuth. *See* June 15 Tr. at 194:7-195:6, (Romansky). Among other things, FCA retains control over user authentication. Chernoby Aff. ¶ 75. And FCA is itself involved in the authorization process for its secure gateways. June 15 Tr. at 101:25-102:3 (Potter).

[9] At one point, Mr. Smith stated that Toyota does not use a gateway for diagnostic data. *See* June 15 Tr. at 129:2-12. The Attorney General then recast that statement to suggest that Toyota does not require any authorization to access its OBD systems. June 16 Tr. at 16:7-12 (Haskell). But under the existing Right-to-Repair Law, independent repair shops need to have the same ability to repair vehicles as dealers, Mass. Gen. L. ch. 93L, § 2(d)(1), which includes the ability to modify vehicle software, *see* June 15 Tr. at 82:23-83:12 (Lowe); June 16 Tr. at 93:17-23 (Garrie). [redacted]

compliance with Section 2 is impossible. *See, e.g.*, June 15 Tr. at 118:11-13, 125:6-9 (Smith).

2. OEMs Must Disable Cybersecurity Controls to Comply with Section 2.

The unrebutted trial testimony established that, to comply with Section 2 of the Data Access Law, OEMs would have to abandon existing cybersecurity controls that protect safety- and emissions-critical functions, and thus help to ensure the safe operation of vehicles within prescribed emissions limits. *E.g.*, June 14 Tr. at 70:6-14, 71:18-72:3, 73:14-22 (Tierney); Chernoby Aff. ¶ 65; Tierney Aff. ¶¶ 13, 90. [redacted] June 14 Tr. at 68:3-11 (Tierney). [redacted] *Id.* at 88:15-16 (Tierney).

[redacted] June 14 Tr. at 68:13-24, 69:4-5 (Tierney). [redacted] *id.* at 68:13-14, [redacted] *id.* at 69:21-22. [redacted] *id.* at 70:6-14 (Tierney), [redacted] *id.* at 71:18-72:3.

[redacted] June 14 Tr. at 73:1-8, 73:24-74:3. To comply with Section 2, GM would have to remove or disable them. *See id.* at 73:14-22.

[redacted] June 14 Tr. at

114:3-10 (Baltes). As Mr. Bort explained, "a secured gateway is there to provide segmentation. It is used as the ability to separate the clean, which is the operation of the vehicle itself, from the dirty, which is the potential of an unknown access[or] source or introduction of any kind of data." *Id.* at 228:18-22. [redacted] *Id.* at 74:15-20 (Tierney). [redacted] *id.* at 74:10-12 (Tierney). To comply with Section 2, GM would have to remove or disable them. *See id.* at 71:18-72:3.[10]

Similarly, FCA would have to remove or disable its cybersecurity controls, *see* Chernoby Aff. ¶ 65—[redacted] *id.* at ¶ 51. As would OEMs generally. *See, e.g.*, Bort Aff. ¶ 93; Garrie Aff. ¶ 64.

3. Disabling Cybersecurity Controls Would Violate Federal Law.

Removing or degrading cybersecurity protections around safety- and emissions-critical vehicle functions would put OEMs out of compliance with federal law. Doing so would frustrate the purposes and objectives of the Safety Act, which established a federal regulatory regime in which both NHTSA and OEMs are obligated to prevent unreasonable risks to safety by conducting recalls, and which NHTSA helps to promote by providing proactive guidance to OEMs to avoid recalls. *See* Dkt. 173, Plaintiff's Trial Brief ("Trial Br.") at 11-15; *see also* U.S. Statement at 2-3, 9 (discussing 49 U.S.C. §§ 30112(a)(3), 30116, 30118).[11] As the United States confirmed, OEMs' obligations extend beyond the requirements specifically laid out in the Safety Act or an FMVSS—

[10] Even if OEMs did not have to physically remove the gateway itself from vehicles, the gateway would not be able to play its role as a firewall protecting individual ECUs from threat actors. *E.g.*, June 14 Tr. at 229:3-22 (Bort).

[11] No expert provided an *immediate* way to comply with Section 2. *See, e.g.*, June 15 Tr. at 185:23-186:8 (Romansky); June 15 Tr. at 118:11-13, 125:6-9 (Smith).

"[a] recall is required based solely on the existence of a safety-related defect, even if no vehicle standard otherwise applies to the defective vehicle component or issue." U.S. Statement at 2 n.4. Those obligations extend specifically to maintaining adequate cybersecurity protections around safety-critical functions. *Id.* at 5-6 (discussing the FCA recall and expressing "concern[] that the Data Access Law potentially creates a similar serious cybersecurity risk to motor vehicle safety").

Removing or degrading existing cybersecurity protections would also violate a specific requirement in the Safety Act. *See* Trial Br. 15-17. The Act prohibits OEMs from "knowingly mak[ing] 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" FMVSS. 49 U.S.C. § 30122(b). And the uncontroverted evidence shows that OEMs have installed cybersecurity protections as elements of design to comply with several FMVSSs, which they would have to remove or degrade to comply with the Data Access Law. Chernoby Aff. ¶¶ 19, 65; Tierney Aff. ¶¶ 26, 90.[12]

Moreover, the cybersecurity protections that OEMs install also help to ensure compliance with stringent federal emissions standards. *See* Tr. Br. 17-18. OEMs would have to remove or degrade these protections to comply with Section 2 of the Data Access Law, which would facilitate third-party access to a vehicle's engine control module to increase vehicle performance at the cost of emissions. *E.g.*, Chernoby Aff. ¶¶ 7-15, 65, 67; Tierney Aff. ¶¶ 28, 82-99, 105-106. Those changes run directly counter to Congress's purposes and objectives in the Clean Air Act. CoL ¶¶ 69-78. And they would run afoul of the Act's "render inoperative provision," 42 U.S.C. § 7522(a)(3)(A). *Id.*

[12] For instance, as Mr. Tierney discussed at trial, removing firmware safeguards, challenge-response mechanisms, and the gateway could allow someone to make changes to the software governing a vehicle's electronic brake control module, manipulating instructions to the vehicle's brake system to modify braking distance or other performance. *See* June 14 Tr. at 89:2-90:4.

B. Section 3 Requires Immediate, Significant Changes.

Section 3 of the Data Access Law requires OEMs to create an "inter-operable, standardized, and open access" "platform" beginning in model year 2022 vehicles. Data Access Law § 3.[13] That platform also must be "[d]irectly accessible by the owner through a mobile-based application." *Id.* It must be "[c]apable of securely communicating all mechanical data emanating directly from the motor vehicle via a direct connection to the platform," *id.*—where "mechanical data" is broadly defined to include "any vehicle-specific data, including telematics systems data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle," *id.* § 1.

Moreover, if the vehicle owner authorizes it, the "mechanical data" emanating from this novel platform must be "directly accessible" to an independent repair facility for the time needed to maintain, diagnose, and repair the vehicle. Data Access Law § 3. And that "access" must be provided on both a read/write basis—so that users will have "the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair." *Id.*[14]

By pegging compliance with Section 3 beginning in model year 2022 vehicles, the requirements were set to take effect almost immediately. *E.g.*, Tierney Aff. ¶¶ 7-8 (model year 2022 vehicles are currently in production and their electric architecture design was completed over two years ago); *see, e.g.*, June 15 Tr. at 51:14-17 (Lowe) (discussing business plan noting that automakers lock in the design of a production model three to five years before release). As with

[13] The Attorney General defines "platform" as the "vehicle architecture and associated software/features." Dkt. 174, Def.'s Proposed Substitute Findings of Fact ("AG FoF") ¶ 60; "inter-operable" as a "standard way to connect and communicate with the vehicle," such that the platform "can be used regardless of the manufacturer," *id.* at ¶ 61); "standardized," as "a common, agreed upon way of communicating," *id.* at ¶ 62; and "open access," as a "a non-gated way to gain access to the [vehicle's] data and capabilities," Smith Aff. ¶ 115.

[14] This "effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle's systems—including braking, steering, and acceleration." U.S. Statement at 7.

Section 2, a manufacturer that does not comply with Section 3 is subject to range of enforcement actions, fines, and private lawsuits. *See* Data Access Law § 5.

1. OEMs Cannot Comply with Section 3 Immediately.

When asked by this Court whether OEMs could provide the inter-operable, standardized, open access platform required by the Data Access Law, every expert agreed that they could not. *See* June 16 Tr. at 41:21 (Smith) ("Definitely not right away."); *id.* at 42:1-3 (Romansky) ("I think the elements of a solution are available, but they're not assembled, and that has not been proven to all work together."); June 15 Tr. at 198:24-199:2 (Romansky) ("I'm not aware of any [telematics systems] that fully comply with Section 3, correct."); June 16 Tr. at 42:7-8 (Bort) ("I don't think we can do that right now."); *id.* at 42:10 (Garrie) ("I agree with my colleagues."). Aside from the platform itself, there is also no "mobile-based application" (Data Access Law § 3) to comply with the law. *E.g.*, June 15 Tr. 95:21-96:17 (Potter); *id.* at 126:13-15 (Smith).

2. OEMs Must Disable Cybersecurity Controls to Comply with Section 3.

As with Section 2, an attempt to comply immediately with Section 3's open access regime for the broadly defined "mechanical data" would require OEMs to remove or disable the same cybersecurity controls that protect safety- and emissions-critical vehicle functions. *See, e.g.*, June 14 Tr. at 72:4-17 (Tierney); Tierney Aff. ¶¶ 90, 99; June 14 Tr. at 126:20-127:10 (Chernoby); Bort Aff. ¶ 78; Garrie Aff. ¶ 90.

3. Disabling Cybersecurity Controls Would Violate Federal Law.

Removing or disabling these key cybersecurity controls would conflict with the purposes, objectives, and requirements of federal law. *See* II.A.3, *supra*; ; *see also* Trial Br. 11-15 (discussing the purposes and objectives of the Safety Act); *id.* at 15-17 (discussing the Safety Act's "make inoperative" provision); *id.* at 17-18 (discussing the Clean Air Act). Indeed, the United States

confirms as much—at least with respect to the Safety Act, by stating that "[t]he open access effectively required by the Data [Access] Law . . . has the potential to cause serious safety problems for motor vehicle owners and to frustrate the ability of motor vehicle manufacturers to follow their obligations to ensure vehicle safety." U.S. Statement at 9.

III. The AG's Purported Solutions Do Not Avoid Preemption.

The Attorney General has proposed a range of purported "solutions"—none of which make it possible for OEMs to meet the Data Access Law's requirements on the timeframe in that law, much less securely. Moreover, her intermediate and longer-term proposals do nothing to resolve the undisputed cybersecurity vulnerabilities in that law—both in Section 2[15] and Section 3.[16]

A. Disabling Telematics Does Not Meet the Requirements of Section 3.

Left with a law with requirements impossible to meet by the deadline imposed in that law, the Attorney General pivots. Her near-immediate "solution" to Section 3 is to negate it. She would have OEMs *avoid* the law by requiring them to get out of the business of telematics altogether. AG Tr. Memo. 16; AG CoL ¶¶ 93-94. By doing so, her witnesses surmise, OEMs could make it so that they "would not be covered by the law." *E.g.*, June 15 Tr. at 32:7 (Lowe). But the question of conflict preemption turns on compliance with a law's substantive requirements, not avoidance of those requirements. That is, preemption analysis "assume[s] compliance with the state-law duty in question." *Geier*, 529 U.S. at 882 (emphasis omitted); *accord, e.g.*, *In re Celexa & Lexapro*

[15] *E.g.*, U.S. Statement Ex. 1, at 2 ("[T]he requirement to establish universal and standardized access requirements increases the scale of risks of any potentially successful cybersecurity attack"); *id.* at 4 ("A non-standardized approach provides cybersecurity benefits such that the scale and potential consequence of any specific cyberattack is inherently reduced. Having more vehicles with a common architecture—especially if that architecture provides a link between external connections and in-vehicle components—means that a single successful malicious cyberattack could have much wider scale of consequences because it can affect a larger number of vehicles.").

[16] *E.g.*, U.S. Statement Ex. 1, at 2 ("NHTSA is . . . concerned about the increased safety-related cybersecurity risks of a requirement for remote, real-time, bi-directional (i.e., read/write capability) access to safety-critical vehicular systems.").

Mktg. & Sales Pracs. Litig., 779 F.3d 34, 40 (1st Cir. 2015) (analyzing conflict preemption claim by looking to whether a party can comply with state requirements). It does not assume avoidance of the law by exiting the relevant market.

The state-law duty in Section 3 is not to disable telematics. Section 3 targets for regulation any "manufacturer of motor vehicles sold in the Commonwealth . . . that utilizes a telematics system"—and then imposes on that regulated manufacturer a requirement to create and deploy "an inter-operable, standardized and open access platform across all . . . makes and models" "[c]ommencing in model year 2022." Data Access Law § 3.

It is undisputed that turning off telematics systems does not create an inter-operable, standardized, and open access platform—much less so by model year 2022. *E.g.*, June 15 Tr. at 31:12-15 (Lowe). And it is well-established that, in assessing whether state law requirements are preempted, a regulated entity's ability to avoid the state law's requirements by ceasing the business operations that make it a regulated entity under that law in the first place plays no part in the preemption analysis. *See, e.g.*, *Mut. Pharm. Co. v. Bartlett*, 570 U.S. 472, 487-88 (2013) (holding that an "actor seeking to satisfy both his federal- and state-law obligations is not required to cease acting altogether in order to avoid liability"). "Indeed," the Court observed, "if the option of ceasing to act defeated a claim of impossibility, impossibility pre-emption would be 'all but meaningless.'" *Id.* (citation omitted).

The Attorney General's "solution" effectively to ban telematics in passenger vehicles would come as a surprise to the voters who passed Section 3. Proponents sold the Data Access Law to Massachusetts voters as a way to provide wider access to vehicle telematics data. *See, e.g.*, AG Tr. Memo. 19-20. Those proponents never told voters that a vote for the ballot initiative was a vote to get rid of telematics—and the many safety and customer-convenience features that come

with them.[17] June 15 Tr. at 32:9-12 (Lowe). The Attorney General's "argument effectively asks [this Court to] circumvent the 'clear intent' of the voters who enacted" the Data Access Law, *see Commonwealth v. Craan*, 469 Mass. 24, 32 (2014) (declining to accord weight to an argument conflicting with the voters' intent in passing a 2008 ballot initiative), and highlights the dormant Commerce Clause problems in the Data Access Law.[18]

B. Telematically Equipped Dongles Are Not a Viable Solution.

The Attorney General's intermediate "solution" is to replace built-in vehicle telematics with telematics on a stick.[19] Voters would doubtless be surprised by this result left unmentioned in the terms of the Data Access Law that they voted for. It would require installing in every passenger vehicle in Massachusetts telematically equipped dongles that would then gather and communicate mechanical data off the vehicle. Smith Aff. ¶¶ 20-24; June 15 Tr. at 119:3-14 (Smith). By her expert's own admission, no dongle with that functionality currently exists. *E.g.*, *id.* at 120:8-10 (Smith).[20] And even if such a telematically equipped dongle were viable, it would take years to agree upon standards for it (as the Data Access Law specifies none), then design, test,

---

[17] Among many other things, telematics systems allow OEMs to ensure that vehicle software is up to date. *E.g.*, Tierney Aff. ¶¶ 6, 36; June 14 Tr. at 90:22-91:6 (Tierney) (observing, based on his experience working with NHTSA at GM, that the agency strongly recommends and supports firmware over-the-air updates because they dramatically increase compliance with safety updates). And at trial, the Attorney General's expert conceded that disabling telematics could potentially have safety consequences. June 15 Tr. at 118:14-18 (Smith).

[18] It is also undisputed that it is a "practical impossibility" for OEMs to disable telematics only for vehicles sold in the Commonwealth. Tierney Aff. ¶ 111. The Attorney General's proposal, then, would be to halt the *nationwide* progression of vehicle telematics technology dead in its tracks—and on a basis that even the voters of just *one* state, the Commonwealth, never intended. A law with "the practical effect [of] control[ling] conduct beyond the boundaries of the state" would be an unconstitutional extraterritorial mandate. *Healy v. Beer Inst. Inc.*, 491 U.S. 324, 336-37 (1989) (observing that the Commerce Clause prevents "the projection of one state regulatory regime into the jurisdiction of another State"). Indeed, it is difficult to see how the complex vehicle architecture changes mandated by the Data Access Law do not project Massachusetts law into every other State.

[19] *E.g.*, AG Tr. Memo. 17; AG CoL ¶ 95; Smith Aff. ¶ 20 (proposing this as a solution to Sections 2 and 3); June 15 Tr. at 117:13-15 (Smith).

[20] The Attorney General's fact witness who supports the use of a dongle solution—and whose tool supplier members manufacturer dongles for sale, June 15 Tr. 98:19-22 (Potter)—likewise does not know if any dongles provide anything even approaching the among of vehicle diagnostic data contemplated by the Data Access Law, *id.* at 99:4-18; *id.* at 99:17-18 ("I don't know the depth of what enhanced diagnostics [dongles] have. I have not studied that.").

and deploy it.[21] And even then, the dongle solution only works if mechanical data is limited to data already available through OBD ports, *see* June 15 Tr. at 125:19-22 (Smith)—an assumption at odds with the Data Access Law's definition of mechanical data, *see* pp. 22, *infra*.[22]

Years from now, when this theoretical dongle is ready, it would be a permanent physical device plugged into the vehicle's OBD port next to a driver's legs. June 15 Tr. 119:3-14 (Smith). The OBD port was never intended to have that type of device plugged into it full time. *Id.* at 119:20-23 (Smith). It would be like permanently affixing to the vehicle a scan tool that a repair shop uses temporarily during active repairs. *Id.* at 144:15-145:15 (Smith).

Unsurprisingly, a telematically equipped dongle brings with it the threat of cybersecurity attack. *See* June 15 Tr. 120:22-24 (Smith). A threat actor could compromise the dongle—through malware or some other means—and then compromise the safety of vehicle. *Id.* at 121:16-23 (Smith). Indeed, dongles are notoriously easy to hack: The Attorney General's expert has personally hacked at least 20 vehicles with dongles. *Id.* at 117:20-118:2 (Smith). And yet Mr. Smith—the proponent of the dongle solution— never conducted any research into any possible long-term harm with having a telematically equipped dongle plugged into a vehicle full time. *Id.* at 119:24-120:2 (Smith).

What is more, the dongle solution would still require OEMs to remove or disable existing cybersecurity protections around safety- and emissions-critical vehicle functions—in contravention of their federal obligations. Bort Aff. ¶¶ 101, 104; Garrie Aff. ¶ 109. Mr. Smith

[21] *See, e.g.*, June 16 Tr. at 53:15-21 (Bort) (discussing steps involved in that undertaking—analyzing the requirements, engineering a solution, acquiring whatever is needed through the supply chain, testing, certifying, and then deploying a telematically equipped dongle); *id.* at 53-9:10 ("[R]ealistically, you're looking at three years.").

[22] The interim solution plays fast and loose with the terms in the Data Access Law in other ways, too. In it, the dongle or the vehicle itself plays the role of the "mobile-based application" through which mechanical data is "[d]irectly accessible by the owner" (Data Access Law § 3). *See, e.g.*, June 15 Tr. at 207:3-208:3. Unsurprisingly, that is not how the Data Access Law's proponents envisioned mobility when fashioning the law and touting it to voters. *See* June 15 Tr. at 29:6-30:7 (discussing how data would go directly from the vehicle to the owner's smartphone).

agreed that OEMs would have to disable their secured gateways entirely or introduce "holes" in the gateway that allow penetration across networks. *See* June 15 Tr. at 122:2-11 (Smith). Currently, the secured gateway provides segmentation between the "clean" side of a vehicle's safety-critical functions and the "dirty" side of telematically accessible ECUs. June 14 Tr. at 228:16-229:2 (Bort); June 16 Tr. at 95:20-96:3 (Bort); *accord* June 14 Tr. at 74:6-2 (Tierney). Nothing would offset the loss of that gateway: After all, dongles usually do not have any cybersecurity protections of their own. June 15 Tr. at 140:21-24 (Smith). The dongle solution, then, would represent a cybersecurity step backward for vehicle telematics.

C. Development of the Section 3 Platform Is Years Away.

For her "long term" solution, the Attorney General finally addresses the actual requirements in Section 3—equipping vehicles with an inter-operable, standardized, open access platform to communicate mechanical data to a mobile-based application. AG Tr. Memo. 17-18; AG CoL ¶¶ 220-28. From an engineering perspective, this is not remotely feasible in the near future, let alone model year 2022.[23] Doing so would require OEMs to make "very substantial physical and electrical changes to [vehicle] architecture," June 14 Tr. at 88:5-7 (Tierney), which cannot safely be accomplished in that timeframe, *see, e.g.*, U.S. Statement at 8.

D. Theoretical Security Standards Do Not Make Compliance Possible.

The Attorney General attempts to fashion a quicker solution to the Data Access Law's requirements by invoking a handful of possible standardized security measures. But none of these

[23] *See* June 14 Tr. at 80:24-81:14 (Tierney) (estimating eight years for compliance—two to three years for standardization, two years to develop electronics and design the platform, two years to design network changes, and then two more years to work with suppliers to produce the platform); Chernoby Aff. ¶ 5 ("FCA generally requires a lead time of at least four years for a new product involving any new electrical architecture. Redesigning the electrical architecture system entirely from the ground up . . . would take several more years."); Bort Aff. ¶ 92 ("The automotive development lifecycle takes at least five years for new product development."); Garrie Aff. ¶ 79 ("[I]t takes approximately 3-8 years to design, verify, validate, test, and implement a component as complex as a gateway.").

would render immediate compliance with the Data Access Law possible. At best, a fully fleshed out security standard would in theory shave off three years from a seven year timeline. June 14 Tr. at 91:14-92:15 (Tierney). And the standards offered by the Attorney General are far from fully fleshed out.

Secure Data Release Model (SDRM). The Attorney General alternatively proposes as an unaffiliated third-party cybersecurity regime something along the lines of the SDRM system developed and run by the National Automotive Service Task Force ("NASTF"), an organization that facilitates dialogue between OEMs and the aftermarket, *see* June 14 Tr. at 10:18-21 (Douglas). *See* AG Tr. Memo.14-15. But SDRM is a limited undertaking not remotely on par with the task of managing access to all vehicle mechanical data. It does not maintain or store any vehicle security information; all of that comes from the manufacturer. Douglas Aff. ¶ 21. It only deals with key codes, not "the breadth of diagnostic repair information that would need to be provided under the Data Access Law." June 15 Tr. at 78:8-10 (Lowe).[24] Essentially, the SDRM verifies that a locksmith is a locksmith. June 14 Tr. at 12:22-13:6 (Douglas). And to get there it took five or six years to develop before launching. *Id.* at 28:1 (Douglas).[25]

Even with the SDRM's limited current scope, it has had its share of cybersecurity problems. Douglas Aff ¶¶ 25-27.; *see also* June 14 Tr. at 27:24-29:11 (Douglas); June 15 Tr. at 79:6-8 (Lowe) ("[W]hen I first joined the board [of NASTF], there were some problems with the way SDRM was first being implemented . . . ."). To take just one example, despite continually

[24] Indeed, even proponents of the Data Access Law have expressed concerns about SDRM. *See* Ex. 20 (ACA official noting in an email to Lowe that "[f]lags raised and alarm bells going off. . . . To be clear, SDRM is not a safe, secure standardized method on accessing vehicles as an equivalent to alternative to SVI."); see June 15 Tr. at 42:12-43:14 (Lowe).

[25] Mr. Douglas has served on the NASTF board since that organization's founding. *Id.* at 10:15-17. He testified that "there's just no possible way that NASTF could maintain that kind of security or that kind of data [to centrally control access]. I mean, we have enough trouble just maintaining the data for a few thousand locksmiths and independent repair shops." *Id.* at 27:20-23.

beefing up security on the SDRM, *see* June 14 Tr. at 27:24-29:11 (Douglas), after the latest update, NASTF still had problems with verified locksmiths lending credentials to individuals not authorized by NASTF to obtain key codes, *see id.* at 29:4-11.

Secure Vehicle Interface (SVI). The Data Access Law's proponents tout SVI as a potential secure solution for managing vehicle data access. In theory, when any data is transmitted off the vehicle, a third-party certificate authority would authenticate who gets the data. June 15 Tr. 38:9-12 (Lowe). But there is no evidence of any manufacturer ever adopting SVI. It is a theoretical set of standards never been tested, confirmed, nor deployed at scale. June 14 Tr. at 79:2-8 (Tierney); *accord* Bort Aff. ¶ 111-12. In fact, Mr. Lowe and his ACA colleagues met with NHTSA for the purpose of gaining the agency's blessing for their SVI solution, a blessing that NHTSA declined to give on the ground that "the establishment of a certificate authority would be extremely difficult and, in their opinion, likely not possible." Ex. 64; June 15 Tr. at 34:5-13 (Lowe). OEMs would have to design completely new data structures, software, and hardware to implement SVI.[26]

Security Credential Management System (SCMS). Mr. Romansky proposes SCMS with a public key infrastructure ("PKI") as a theoretical way to address the risks of standardized access controlled by a single entity. Romansky Aff. ¶¶ 55-57. But as with the other proposals, it is not nearly ready for showtime. It lacks the necessary infrastructure for implementation and has never been tested for use with diagnostic data let alone on the scale required. Bort Aff. ¶ 112. No OEMs use SCMS for maintenance, diagnosis, or repair. June 15 Tr. 193:21-23 (Romansky).

Vehicle-to-Everything (V2X). Relatedly Mr. Romansky also posited that V2X could play a role in how an unaffiliated entity could communicate vehicle data. Romansky Aff. ¶¶ 33-41. But,

[26] Garrie Aff. ¶ 114; *see also* June 15 Tr. 102:14-104:22 (Potter) (agreeing that before SVI could be employed, several steps would have to happen—OEMs would have to design new software for gateways, tool manufacturers would have to rewrite diagnostics, the two would have to get together and agree on mapping programs between the two, following by designing, testing, and implementing new software that is consistent with a new standardized policy).

like the others, it is nowhere near ready to serve as a solution to the Data Access Law. Mr. Romansky conceded that he is unaware of any manufacturer that has used or even attempted to use V2X to grant access to its OBD systems or authorize tools—let alone to serve as an unaffiliated entity to transmit data. June 15 Tr. at 193:2-17, 193:21-23. Moreover, there have been concerns about the amount of bandwidth allocated to V2X. June 16 Tr. at 95:4-95:8 (Garrie). And the FCC recently reduced the amount of spectrum allocated for V2X. *See id.* at 95:1-3 (Garrie); *see also* FCC 20-164, First Rpt. & Order (Nov. 20, 2020), at https://www.fcc.gov/document/fcc-modernizes-59-ghz-band-improve-wi-fi-and-automotive-safety-0.

E. The Attorney General Offers Implausible Interpretations of the Law.

Even under the Attorney General's construction of terms in the Data Access Law, OEMs cannot comply with Sections 2 or 3 on the timeline required by that law without running afoul of their federal safety and emissions obligations. *See* II, *supra*. There is no need to go further.

But the hypothetical "solutions" offered by the Attorney General's experts for how OEMs might at some later date hypothetically be able to comply suffer from another fatal flaw: they rely on a narrow reading of the Data Access Law that is flatly contradicted by its plain language.[27]

Under Massachusetts law, the "duty of statutory interpretation is one for the courts." *Police Comm'r of Boston v. Cecil*, 431 Mass. 410, 413 (2000). Statutory language is to be interpreted according to its "ordinary language." *Commonwealth v. Daley*, 463 Mass. 620, 624 (2012); *accord Boss v. Town of Leverett*, 484 Mass. 553, 557 (2020) ("A fundamental tenet of statutory

[27] The experts in the hot tub fell victim to the same temptation—unsurprisingly, given the convoluted language in the Data Access Law. *Cf.* June 16 Tr. at 66:6-10 (Romansky) ("I have a strong desire to want to start to invent and create [] whole new solutions which don't necessarily tie to the law, which to your point earlier is not helpful, so I'll try to refrain from going down that path."). During the hot tub, Mr. Smith repeatedly referred to the Uniform Data System ("UDS"), which only deals with traditional repairs that dealerships (and thus, under the 2013 Right to Repair Law, independent repair facilities) already make. *See id.* at 13:56-8, 57:2-25, 79:14-18, 103:10-14 (Smith). UDS does not come close to providing the broad read-write functions required in the Data Access Law. *Id.* at 68:13-69:4 (Bort).

interpretation is that statutory language should be given effect consistent with its plain meaning.") (internal quotation omitted).[28]

Massachusetts courts accord some deference to agencies charged with enforcement. *See, e.g.*, *Mass. Coal. for Homeless v. Dep't of Transitional Assistance*, 2000 WL 776564, at *6-7 (Mass. Super. Ct. June 1, 2000). But "this principle is one of deference, not abdication." *Leopoldstadt, Inc. v. Comm'r of Div. of Health Care Fin. & Policy*, 436 Mass. 80, 91 (2002). The deference accorded an agency on account of its enforcement powers only applies to the extent the agency's interpretation is "not inconsistent with the plain language of the statutory provisions." *Smith v. Winter Place LLC*, 447 Mass. 363, 367-68 (2006); *accord Pub. Empl. Ret. Sys. of Ohio v. Betts*, 492 U.S. 158, 171 (1989) ("[N]o deference is due to agency interpretations at odds with the plain language of the statute itself.").[29]

Several of the Attorney General's interpretations conflict with the plain language of the statute. Indeed, she purports to read entire terms or phrases out of the law.

Vehicle Networks. Section 2 contemplates, as an alternative to abandoning manufacturer authorization outright, an independently administered "authorization system for access to *vehicle networks and their on-board diagnostic systems*" that is "standardized across all makes and models sold in the Commonwealth." Data Access Law § 2 (emphasis added). The plain language of the statutory provision thus encompasses not only "on-board diagnostic systems" but also "vehicle networks" of which on-board diagnostic systems are only a part. *Id.*

Yet the Attorney General attempts to avoid the direct conflict between federal law and

[28] The standards mirror those in federal court. *See, e.g.*, *United States v. Cortes-Caban*, 691 F.3d 1, 16 (1st Cir. 2012) ("As with any question of statutory interpretation, our analysis begins with the plain language of the statute.").

[29] Agency deference is premised at least in part on "the agency's experience, technical competence, and specialized knowledge." *Souza v. Registrar of Motor Vehicles*, 462 Mass. 227, 229 (2012). When the agency lacks "any special competence to determine what the Legislature [or voters] meant" by a term "unrelated to the[] subjects" over which it has "specialized knowledge," "the interpretive question . . . is a purely legal one" for the Court. *Id.*

Section 2 of the Data Access Law by reading the reference to "vehicle networks" as synonymous with OBD systems. AG Tr. Memo. 14; AG CoL ¶ 80; *see also* June 15 Tr. at 124:5-12 (Smith) (reading "vehicle networks" no broader than a vehicle's OBD system); *id.* at 188:22-189:9 (Romansky) (opining only on OBD systems for Section 2). That violates basic rules of statutory construction. *See, e.g.*, *Tamulevich v. Robie*, 426 Mass. 712, 713-14 (1998) (declining to construe two different terms in a statute as synonymous because, by including both, "the Legislature would not likely have used them to mean the same thing").

As Mr. Romansky admitted, vehicle networks and on-board diagnostic systems are different things that serve different roles in a vehicle. June 15 Tr. at 187:8-25 (Romansky). A vehicle network is a communication network within a vehicle, and any given vehicle might have multiple vehicle networks separated by gateways or firewalls. *Id.* at 186:9-187:4 (Romansky).

Mechanical Data. The Attorney General takes a similarly narrow reading of the mechanical data that the Data Access Law targets. *E.g.*, AG CoL, at ¶¶ 36-38. But the statute defines "[m]echanical data" 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." Data Access Law § 1 (emphasis added). By its plain terms, that data is broader than that merely "used" for diagnosis, repair, or maintenance. Indeed, Mr. Lowe—who helped draft the ballot language and whose organization was heavily involved in the initiative process, *see* June 15 Tr. at 13:5-12—confirmed that the "otherwise related to" language was intended as a "catch-all" precisely so that there would not be a narrow interpretation, *see id.* at 24:3-6. And it is a longstanding principle of Massachusetts law that "none of the words of a statute is to be regarded as superfluous, but each is to be given its ordinary meaning." *Commonwealth v. Woods Hole, Martha's Vineyard and Nantucket S.S. Auth.*, 352 Mass.

617, 618 (1967) (internal quotations and alterations omitted).[30]

Indeed, if the only data at issue were repair data on vehicle OBD systems plus telematics, *see, e.g.*, AG CoL ¶¶ 36-38, then Section 2 of the Data Access Law would be superfluous and add nothing to Chapter 93K. Section 3 adds telematics data. But Section 2 does not mention telematics. And under existing Massachusetts law, OEMs were already obligated to provide, through the OBD, access to all vehicle data necessary for diagnosis, repair, or maintenance. *See* Mass. Gen. Laws ch. 93K, § 2(d)(1) (2013 Right to Repair Law); Potter Aff. ¶¶ 10-11; Tierney Aff. ¶ 78.

Manufacturer Involvement. Section 2 both mandates standardization and proscribes "*any* authorization by the manufacturer, *directly or indirectly*" to OBD systems, unless there is standardized access to all vehicle networks across all vehicles sold in the Commonwealth. Data Access Law § 2 (emphasis added). Though of course OEMs must engage with the entity that would take over the role of authorizing access to OBD systems, *see* June 16 Tr. 61:21-62:2 (Court), once that relationship is established, the plain language of the statute prohibits OEMs from exercising any kind of day-to-day control over who is authorized to access their OBD systems.[31]

Authorization and Authentication. Finally, the Attorney General asserts that the Data Access Law reaches only manufacturer authorization, not manufacturer authentication, and that authorization and authentication are separate things. AG Tr. Memo. 12-13; AG CoL ¶¶ 40-43. Her own expert disagrees with that reading.[32]

---

[30] The ordinary meaning of "otherwise related to" creates a "broadly worded" obligation that extends beyond the terms modified by that language. *See, e.g., Khan v. Parsons Glob. Servs.*, Ltd., 521 F.3d 421, 423 (D.C. Cir. 2008).

[31] After all, the phrase "directly or indirectly" evinces a "broad" prohibition on manufacturer involvement in the authorization process. *See, e.g., Burley v. Comets Cmty Youth Ctr., Inc.*, 75 Mass. App. Ct. 818, 821 (2009) (quoting *N. Am. Expositions Co. Ltd. P'ship v. Corcoran*, 452 Mass. 852, 862 (2009)); *accord Manning v. Zuckerman*, 388 Mass. 8, 14 (1983) (describing "directly or indirectly" as "broad language") (internal quotations omitted).

[32] Romansky Aff. ¶ 28 ("Vehicles that fully comply with the 2020 Right to Repair Law will need to support authentication and authorization of a broad array of different users and diagnostics tools."); June 16 Tr. at 44:14-18 (Romansky) ("I think section 2 establishes a common authentication authorization mechanism[.]"); June 15 Tr. at 193:24-194:6 (Romansky) (agreeing that both of his proposed solutions to Section 2 involve having authentication

There is no basis to separate the two concepts. Authorization and authentication work in tandem. June 14 Tr. at 211:3 (Bort). Authorization deals with the scope of access—*e.g.*, how many doors a key can open—while authentication deals with identifying the unique person who would get the key to that access. *See id.* at 210:14-211:1 (Bort). Any ability to authenticate users without the ability to authorize users in the first place would be meaningless. *Id.* at 211:6-8 (Bort).

As the Attorney General observed in another pleading, courts should "'take note of terms that carry technical meaning[s],' including 'when interpreting a statute about computers.'" Dkt. 204, Def.'s Mot. for Judgment as a Matter of Law (quoting *Van Buren v. United States*, 141 S. Ct. 1648, 1657 (2021)). Indeed, they should. The *Van Buren* Court recognized that the concept of "authorized access," as a technical matter, "contemplates a specific type of authorization—that is, authentication, which turns on whether a user's credentials allow him past a computer's access gate." 141 S. Ct. at 1659 n.9) (internal quotations omitted). The technical meaning of authorization in the computing world *subsumes* a process of authenticating a user to grant access. *Id.* (noting that A Dictionary of Computing defines "'authorization' as a 'process by which users, having completed an . . . authentication stage, gain or are denied access to particular resources based on their entitlement.'"). At the very least, there is no basis to decouple the interrelated concepts of authorization and authentication.

IV. The Data Access Law's Provisions Are Inseverable.

The Data Access Law must rise or fall as a whole. The question of severability is "a matter of state law." *Leavitt v. Jane L*, 518 U.S. 137, 139 (1996). Under Massachusetts law, the Data Access Law's provisions are inseverable from one another. Notably, the law contains no

services provided by an independent organization). Nor does it make sense to decouple the "open access" requirement in Section 3 from the no-manufacturer-authorization access requirement in Section 2. *See, e.g.*, U.S. Statement at 8 ("Reading Sections 2 and 3 of the Data Access Law together, a motor vehicle manufacturer may not implement controls over remote access to any systems . . . unless those controls are administered by an unaffiliated third party.").

severability clause—and even if it did, Massachusetts has never enforced such a clause in a ballot initiative. *See, e.g., Abdow v. Atty. Gen.*, 468 Mass. 478, 509 (2014); *see also Mass. Teachers Ass'n v. Sec'y of Com.*, 384 Mass. 209, 233 (1981). There is a good reason why. "The mandate that an initiative petition contain a single 'common purpose' arises because a voter, unlike a legislator, has no opportunity to modify, amend, or negotiate the sections of a law proposed by popular initiative." *Anderson v. Atty. Gen.*, 479 Mass. 780, 785 (2018) (internal quotations omitted). A voter "cannot sever the unobjectionable from the objectionable, and must vote to approve or reject an initiative petition in its entirety." *Id.* (internal quotations omitted). Thus, there is no way of discerning whether voters would have approved Section 2 or Section 3 standing alone.

Moreover, Sections 2 and 3 of the law do not operate wholly independently of each other. The Attorney General's expert agreed that the two "build on each other" to accomplish the intended vehicle data access. June 16 Tr. at 44:14-18 (Romansky) ("On the pieces of the law, section 2, section 3, I think they build on each other. I think section 2 establishes a common authentication authorization mechanism, then section 3 takes advantage of that and says it's extended to telematics."). Thus, even under the broader principles of severability intended for legislatively enacted statutes, the two provisions cannot be severed. *See, e.g., In re Op. of the Justices to the Senate*, 436 Mass. 1201, 1213 (2002) (holding provisions inseverable because they do not operate entirely "independently" of each other; one could not be stricken without "undermining the integrity and purpose" of the law as a whole).

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court (1) find in its favor on Counts I and II of its Complaint; (2) declare that the Data Access Law is unenforceable as preempted by the Safety Act and Clean Air Act; (3) permanently enjoin enforcement of the Data Access Law; and (4) grant any such further relief as the Court deems appropriate.

Dated: June 23, 2021

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

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

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and that paper copies will be sent to those indicated as non-registered participants on June 23, 2021.

/s/ Laurence A. Schoen