UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. ANDREA CAMPBELL, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendants.	CIVIL ACTION NO. 1:20-cv-12090-DPW

DEFENDANT'S MEMORANDUM IN OPPOSITION TO PLAINTIFF'S EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AND EMERGENCY HEARING

On March 7, 2023, the Attorney General filed a notice (ECF #330) in which she announced her intention, as of June 1, to terminate her previous stipulation not to enforce the Commonwealth's Data Access Law. "The people of Massachusetts," she wrote, "deserve the benefit of the law they approved more than two years ago." ECF #330 at 4.

That the Data Access Law would one day come into enforcement should come as no surprise. Indeed, as early as January 27, 2021, this Court warned the members of plaintiff Alliance for Automotive Innovation, "I really mean it about, if their business planning is not including thinking about [the Data Access Law] coming into play at some point, then they're whistling by the graveyard on it." ECF #94 at 39-40. Nonetheless, waiting until three business days before June 1,[1] the Alliance filed an "Emergency Motion for Temporary Restraining Order and Expedited Hearing," ECF #339, and this Court scheduled a hearing.

[1] The Alliance filed its motion shortly before 8:00 P.M. on Thursday, May 25—which, under District Court Local Rule 5.4(d), is considered a filing on the following day. And Monday, May 29, of course, was the Memorial Day holiday.

At the outset, it should be clearly understood what the Alliance is requesting: Not a TRO, but rather an injunction. The circumstances of its motion are indistinguishable from those that would surround any motion for a preliminary injunction: The Attorney General received notice of the Alliance's motion, both parties are receiving an opportunity to participate in argument on that motion, and both parties have filed extensive memoranda regarding the motion. And the Alliance seeks an order of indeterminate duration, specifically, "until the Court renders a judgment in the instant action, or at least until the Court can consider a preliminary injunction requesting such relief." ECF #339 at 1.

But there has never been a basis to enjoin enforcement of the Data Access Law, and there certainly is not one now. The Alliance does not have standing, and it does not have a cause of action. Furthermore, there is not even the slightest conflict between the Data Access Law and federal law. NHTSA's vehicle safety standards simply do not cover the cybersecurity issues upon which the Alliance rests its preemption case. And the Clean Air Act expressly requires that auto manufacturers share "any and all information" regarding emission-related diagnoses and repairs to "any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines"—precisely the sort of access that the Alliance seeks to block here. 42 U.S.C. § 7521(m)(5).

Nor is there any "emergency" here, let alone one that is not of the OEMs' own making. *See Respect Maine PAC v. McKee*, 622 F.3d 13, 16 (1st Cir. 2010) (denying emergency motion for injunctive relief from state campaign finance laws, where plaintiffs waited until shortly before affected election to seek relief; "this 'emergency' is largely one of their own making"). The Data Access Law has been in effect, and privately enforceable, since December 2020. The OEMs have been obligated to comply with it, and several have done so. Other OEMs, like the two so-called "representative" OEMs, GM and Stellantis, have adamantly refused to make any

effort to comply with the Law. But the fact that the Attorney General previously agreed to refrain from taking the action required of her under the Law and from otherwise enforcing the Law—at this Court's request and with the understanding that doing so would give the Court a reasonable time to bring "this case to an appealable final judgment," ECF #243—does not excuse their failure. The OEMs' refusal to take any steps to come into compliance with the Law in the 30 months since it was enacted is not irreparable harm, nor should this Court be in the business of rewarding such obstinance with injunctive relief.[2]

"To obtain a preliminary injunction, the plaintiffs bear the burden of demonstrating (1) a substantial likelihood of success on the merits, (2) a significant risk of irreparable harm if the injunction is withheld, (3) a favorable balance of hardships, and (4) a fit (or lack of friction) between the injunction and the public interest." *Nieves-Marquez v. Puerto Rico*, 353 F.3d 108, 120 (1st Cir. 2003). The last two factors "merge when the Government is the opposing party." *Nken v. Holder*, 556 U.S. 418, 435 (2009). The first factor—likelihood of success on the merits—is the "'sine qua non' of a preliminary injunction." *Arborjet, Inc. v. Rainbow Treecare Sci. Adv.*, Inc., 794 F.3d 168, 173 (1st Cir. 2015) (citations omitted). "[T]he movant, by a clear showing, carries the burden of persuasion." *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997). Because the Alliance cannot carry its burden on any of these factors, its motion should be denied.

I. THE ALLIANCE DOES NOT HAVE A LIKELIHOOD OF SUCCESS ON THE MERITS OF ITS TWO REMAINING CLAIMS.

The Court has properly dismissed most of the Alliance's claims. ECF #334. The two that remain are the Alliance's preemption claims under the Federal Motor Vehicle Safety Act

[2] What's more, the relief the Alliance now requests—an order "prohibiting enforcement of the . . . Data Access Law," ECF #339 at 1—would, for the first time, effectively release manufacturers from their obligations under the law and bar even enforcement of the law by private parties whom the law empowers to seek enforcement and who are not party to this suit. *See* Mass. G.L. c. 93K, § 6(b); Fed. R. Civ. P. 65(d)(2).

("MVSA") and Clean Air Act ("CAA"). The Alliance does not have a likelihood of success on the merits of either claim. To the contrary, both claims fail for lack of associational standing, lack of a cause of action, as a matter of law, and because the evidence submitted at and after trial confirms that OEMs can securely comply with the Data Access Law without violating federal law.

A. The Alliance Does Not Have Associational Standing.

The Alliance lacks associational standing to assert preemption claims on behalf of its members, where the evidence has shown that OEMs can and have taken different approaches to complying with the Data Access Law and some are already in compliance. ECF #232 at CL ¶¶ 1-10; ECF #263 at 15-19. The Alliance has failed to establish that "both the asserted claim[s] and the requested relief can be adjudicated without the participation of individual members as named plaintiffs." *Me. People's Alliance & Nat. Res. Def. Council v. Mallinckrodt, Inc.*, 471 F.3d 277, 283 (1st Cir. 2006).

In an attempt to establish associational standing, and over the Attorney General's objection, the Alliance initially proposed that four OEMs – GM, Toyota, Mercedes-Benz, and FCA (now called Stellantis) would constitute "representative" OEMs for purposes of its preemption claims. But the Alliance then arbitrarily chose to remove two of the four, Mercedes-Benz and Toyota, from its selection of representative OEMs. ECF #131-1 at 20:3-9. Even with respect to the remaining two, application of the Data Access Law involves materially "different factual scenarios." *Nat'l Ass'n of Gov't Employees*, 914 F. Supp. 2d 10, 14 (D. Mass. 2012). The Alliance did not provide evidence that GM and Stellantis's approach to cybersecurity and data access is representative of automobile manufacturers in general. Nor did it prove that, industry-wide, OEMs are similarly situated in their vehicle design and ability to comply with the law. To the contrary, the evidence at trial showed that "member circumstances differ" with respect to OEMs' vehicle design and ability to comply with the Data Access Law. *Pharm. Care*

Mgmt. Ass'n v. Rowe, 429 F.3d 294, 314 (1st Cir. 2005). For example, the evidence showed only certain OEMs, like FCA, use a secure gateway, while other OEMs, like Toyota, do not and are therefore able to comply with Section 2 now. Tr. II:108-09, 129. Similarly, the Alliance's expert Daniel Garrie explained that it is "not necessarily the case today" that "all OEMs are using telematics" – testimony that shows that some OEMs can comply with Section 3 now. Tr. III:73; *see also* ECF #262 (Joint Stipulation of the Parties).

Any injunctive or declaratory relief awarded in favor of the Alliance would not "inure to the benefit" of all the Alliance's members because, due to their different vehicle architectures and underlying technology, those members differ in the ease with which they can comply with the Data Access Law. *Pharm. Care Mgmt. Ass'n*, 429 F.3d at 306. Where, as in this case, the Court would have to "review the individual circumstances" of different manufacturers' technical capabilities to assess the Alliance's claims of conflict preemption, associational standing is improper. *Nat'l Ass'n of Gov't Employees*, 914 F. Supp. 2d at 14. This Court thus lacks jurisdiction to address the Alliance's preemption claims.

B. The Alliance Does Not Have a Cause of Action.

The Supremacy Clause "does not create a cause of action," *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 325 (2015), nor is any claim based on the Supremacy Clause "cognizable under 42 U.S.C. § 1983," *Boston & Me. Corp. v. Town of Ayer*, 330 F.3d 12, 18 (1st Cir. 2003). To invoke the equitable powers of an Article III court, a plaintiff seeking to establish that federal law immunizes it from state regulation must identify a substantive "federal right that [it] possesses against" the defendant. *Va. Office for Prot. & Advocacy v. Stewart*, 563 U.S. 247, 260 (2011). Here, the Alliance has failed to identify any substantive federal right conferred on an OEM by the MVSA or CAA that is enforceable against states or state officials sued in their official capacity. CL ¶¶ 10-16.

To the contrary, both the MVSA and the CAA evince Congress's "intent to foreclose" the equitable relief requested by the Alliance in this case. *Armstrong*, 575 U.S. at 328 (internal quotation marks omitted). The purportedly preemptive sections of the MVSA cited by the Alliance – the recall notice provisions in 49 U.S.C. §§ 30118-30120 and the "make inoperative" provision in 49 U.S.C. § 30122(b) – are enforceable by the Secretary of Transportation, not by private individuals through an individual right of action. Similarly, the would-be preemptive provision of the CAA cited by the Alliance – the "render inoperative" provision in 42 U.S.C. § 7522(a)(3)(A) – likewise provides an exclusive right of action to the United States to enforce the provision through civil litigation. *See* 42 U.S.C. § 7523(a)-(b). As the Supreme Court has explained, "the 'express provision of one method of enforcing a substantive rule suggests that Congress intended to preclude others.'" *Armstrong*, 575 U.S. at 328 (quoting *Alexander v. Sandoval*, 532 U.S. 275, 290 (2001)); *see also Thorne v. Pep Boys Manny Moe & Jack Inc.*, 980 F.3d 879, 892 (3d Cir. 2020) (the MVSA "favor[s] public over private enforcement").

C. The Alliance's Claims Fail as a Matter of Law Because There Is No Conflict Between the Data Access Law and Federal Law.

As plaintiff, the Alliance has the burden to prove preemption. *Capron v. Office of Att'y Gen'l*, 944 F.3d 9, 13, 21 (1st Cir. 2019) (citation omitted), *cert. denied*, 141 S. Ct. 150 (2020). In implied preemption cases like this one, courts presume that "the historic police powers of the States" are not superseded "unless that was the clear and manifest purpose of Congress." *Arizona v. United States*, 567 U.S. 387, 400 (2012) (citation omitted). This presumption reflects the fact that "the States are independent sovereigns in our federal system," as well as "the historic primacy of state regulation of matters of health and safety." *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996) (citation omitted).

Recent rulings by the Supreme Court have made clear that a preemption claim must be "grounded 'in the text and structure of the statute at issue.'" *Kansas v. Garcia*, 140 S. Ct. 791, 804 (2020) (citation omitted). Policy preferences and "brooding federal interest[s]" are insufficient to preempt state law. *Va. Uranium, Inc. v. Warren*, 139 S. Ct. 1894, 1901 (2019) (lead opinion of Gorsuch, J.). Rather, "only federal laws 'made in pursuance' of the Constitution, through its prescribed processes of bicameralism and presentment, are entitled to preemptive effect." *Id.* at 1907.

The Alliance argues that the Data Access Law is preempted by a handful of federal motor vehicle safety standards ("FMVSS") that govern acceleration, braking, steering, and air bag systems because certain OEMs have "installed a variety of cybersecurity protections" around those "regulated vehicle functions." ECF #340 at 6. But an FMVSS impliedly preempts state law only if that law stands as an "'obstacle' to the accomplishment" of a "significant" objective of the federal regulation, *Williamson v. Mazda Motor of Am., Inc.*, 562 U.S. 323, 330 (2011) (quoting *Geier v. Am. Honda Motor Co.*, 529 U.S. 886 (2000)), and none of the FMVSS cited by the Alliance even mentions cybersecurity protections, much less adopts a significant federal objective on cybersecurity that is incompatible with the Data Access Law. As NHTSA itself has acknowledged, vehicle cybersecurity "is not covered by an existing Federal Motor Vehicle Safety Standard." ECF #232 at CL ¶ 77. *See Sprietsma v. Mercury Marine*, 537 U.S. 51, 65 (2002) (agency's "decision not to regulate" particular safety issue "is fully consistent with an intent to preserve state regulatory authority pending the adoption of specific federal standards"); *Freightliner Corp. v. Myrick*, 514 U.S. 280, 289 (1995) ("it is not impossible for" a party "to comply with both federal and state law" when "there is simply no federal standard" for that party to comply with).

Nor does the Data Access Law conflict with the "make inoperative" provision of the MVSA, 49 U.S.C. § 30122(b), such that it is impossible for an OEM to comply with both the state law and the MVSA. *See* ECF #340 at 6. Section 30122(b) provides that OEMs and others "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." The Data Access Law does not require removing or disabling safety equipment or features installed to comply with a motor vehicle safety standard. Further, because no motor vehicle safety standard covers vehicle cybersecurity or data access controls, cybersecurity features are not "part of a device or element of design installed . . . in compliance with an applicable motor vehicle safety standard." Section 30122(b) does not preempt state laws that impact features that OEMs choose to layer on top of safety equipment required by vehicle safety standards, but to which the standards do not apply. ECF #232 at CL ¶¶ 91-101.

As for the Alliance's rehash of its CAA preemption claim, *see* ECF #340 at 8-9, the statute and its regulations make clear that it is the purpose of Congress to *require*, rather than prohibit, open access to emissions-control data. *See* 42 U.S.C. § 7521(m)(5) (directing EPA to require OEMs to provide to "any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines . . . any and all information needed to make use of the [vehicle's] emission control diagnostic system . . . and such other information including instructions for making emission-related diagnoses and repairs"); *see also* 40 C.F.R. § 86.1808-01(f)(2)(i); 40 C.F.R. § 86.010-38(j)(3)(i). There is no other provision in the CAA or its regulations that regulates vehicle cybersecurity or data access controls. And the CAA's savings clause expressly preserves the right of states "to control, regulate, or restrict the use, operation, or movement of registered or licensed motor vehicles." 42 U.S.C. § 7543(d). By seeking to standardize access to vehicles' on-board diagnostic systems, the Data Access Law falls well within the saving clause's

preservation of state authority to regulate anything that "affects the vehicle's 'quality' and 'method' of functioning (*i.e.*, operation)." *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, & Prods. Liab. Litig.*, 959 F.3d 1201, 1216 (9th Cir. 2020) (citation omitted), *cert. denied*, 142 S. Ct. 521 (2021).

D. The Alliance Has Failed to Prove that There is "No Set of Circumstances" Under which an OEM Can Comply with Both State and Federal Law.

Lastly, even if there were a potential conflict, the Alliance failed to satisfy its burden of proving that there is "no set of circumstances" under which any OEM can comply with both state and federal law. *NCTA – The Internet & TV Ass'n v. Frey*, 7 F.4th 1, 17 (1st Cir. 2021); *see also CDK Glob. LLC v. Brnovich*, 16 F.4th 1266, 1275 (9th Cir. 2021) ("[F]or purposes of a facial challenge, the current design of the system is irrelevant – [the plaintiff] must show that no set of circumstances exists under which the [state law] could be valid."). To the contrary, the evidence at trial showed that OEMs can securely comply with the Data Access Law without violating federal law. Some OEMs are already in compliance, and others can comply with the law if they devote the resources and time to make appropriate changes to their vehicles' architectures. *See* ECF #217 at 2-15; ECF #232 at FF ¶¶ 50-74, 171-245, CL ¶¶ 82-89, 94-101.

Importantly, these critical points were admitted by the Alliance's own experts. Throughout this case, the Alliance has deployed a strategy of interpreting key provisions in the Data Access Law extremely broadly and then arguing that the law, so interpreted, conflicts with federal law. *See*, *e.g.*, Tr. I:126 (testimony of FCA's Mark Chernoby that, where he viewed language in the Data Access Law as vague or ambiguous, he had "to interpret it in the broadest form"); Tr. I:187-88 (testimony of Alliance's expert Bryson Bort that he interprets the term "mechanical data" (as used in Section 3) to encompass, among other things, (i) all ECUs' firmware, (ii) all manner of internal messages that concerned the vehicle's operation, and (iii)

diagnostic functions that are reserved for engineering and manufacturing). There are, of course, legal flaws with that strategy: It flies in the face of the Supreme Court's admonition that state laws must be "read to avoid [preemption] concerns" whenever possible, *Arizona*, 567 U.S. at 413-15, and disregards the "great weight" that must be accorded to the Attorney General's limiting construction of state law. *McGuire v. Reilly*, 386 F.3d 45, 55, 64 (1st Cir. 2004), *Nat'l Org. for Marriage v. McKee*, 649 F.3d 34, 66 (1st Cir. 2011).

But the wheels really came off that strategy at trial—and particularly during the expert "hot tub" conducted by this Court—when the Alliance's experts repeatedly conceded that, under the more reasonable interpretations of the Data Access Law advanced by the Attorney General's evidence, OEMs could readily implement the Data Access Law without violating federal law. For example, after hearing the Attorney General's expert Craig Smith testify that he understood "mechanical data" to require not access to all vehicle data, but rather just a "level playing field" with respect to data used by automotive dealerships to diagnose, maintain, and repair vehicles,[3] Tr. III:55-56, the Alliance's Mr. Bort conceded that "that's a different scope, and I wouldn't have an issue with that," Tr. III:79. The Alliance's other expert, Daniel Garrie, agreed that, when the Law is interpreted in a more pragmatic fashion, "[i]t seems a lot more feasible." Tr. III:58. Similarly, Bort initially testified that he interpreted the term "open access" in Section 3 to mean that "anyone can have access to the insides of a vehicle." Tr. I:189. His opinion of the risks posed by the Data Access Law flowed from his view that the required level of access includes "the potential to reprogram and do firmware and software development." Tr. III:68-69. At the hot tub, however, Bort conceded that, under the more pragmatic interpretation advanced by the Attorney General's experts, their solutions were "not far-fetched," Tr. III:70-71, and

[3] The only understanding that is consistent with the Law's plain language, context, and purpose. *See* ECF #292 at 15-16.

would involve only "a minor level of doing that risk assessment and potential rearchitecture," which he "wouldn't anticipate . . . being an exponentially burdensome piece," Tr. III:75.

The hot tub exposed the failures of the Alliance's trial strategy and established that its claims cannot survive reasonable interpretations of the Data Access Law. Nevertheless, now—two years after trial—the Alliance has reverted to the same strategy, claiming that OEMs "cannot fully comply with the Data Access Law" (even though some OEMs are already in compliance) and asserting OEMs will "need years to design, build, and test vehicles" that comply with the Law (even though the "representative" OEMs GM and Stellantis have steadfastly refused to make any attempt to comply with the law since it took effect in 2020). *See* ECF #340 at 13. The Alliance's request for an injunction at this late stage is unsustainable under the law on federal preemption, the trial record, and basic principles of equity.

II. THE ALLIANCE HAS FAILED TO SHOW THAT ABSENT AN INJUNCTION ITS MEMBERS WILL SUFFER IRREPARABLE HARM.

The Alliance argues that if required to comply with the Data Access Law, OEMs will suffer three forms of harm: (1) OEMs will "have to alter their vehicles in a manner that would increase the cybersecurity risks to safety- and emissions-critical vehicle systems," which would result in "federal scrutiny, enforcement, and penalties, as well as enormous potential recall and repair costs if compliance with the Data Access Law renders vehicles' safety and emissions systems defective."; (2) if the OEMs opted to comply by disabling the telematics systems in their vehicles, some of the vehicle features would be limited; and (3) if the OEMs opted to comply by disabling the telematics systems in their vehicles, this "likely could not be cabined just to Massachusetts residents" and some OEMs may need to withdraw from the Massachusetts market altogether. ECF #340 at 10-11.

These asserted harms are affirmatively refuted by the trial record and insufficient to justify an injunction. This is especially true here, where the Alliance has no likelihood of success on the merits. *New Comm Wireless Servs., Inc. v. SprintCom, Inc.*, 287 F.3d 1, 8-9 (1st Cir. 2002) (likelihood of success is the "sine qua non" of preliminary-injunction analysis; without it, remaining factors become "matters of idle curiosity").

First, each of the harms alleged by the Alliance is impermissibly speculative. *Ross-Simons of Warwick, Inc. v. Baccarat, Inc.*, 102 F.3d 12, 19 (1st Cir. 1996) ("[A] preliminary injunction is not warranted by a tenuous or overly speculative forecast of anticipated harm."). Indeed, the notion that OEMs would have to alter vehicles in a manner that would increase cybersecurity risks is not only speculative—it was refuted by the Alliance's own experts at trial, when they acknowledged that safe compliance with the Data Access Law was possible, and by evidence that two OEMs, Subaru and Kia, have made changes to comply with the Law since 2021. *See* ECF #217 at 9-15; ECF #262; ECF #263; ECF #263-1. There is no evidence that Subaru and Kia have been subject to any "federal scrutiny, enforcement, and penalties," or "recall and repair costs"; to the contrary, the Alliance stipulated that "Subaru vehicles that are not enrolled in the [telematics] system are safe" and that "[a]s of the time such vehicles are sold to consumers, they comply with all applicable [FMVSS], as well as the Clean Air Act and all applicable regulations promulgated thereunder." ECF #262 ¶ 6. The Alliance's speculative claims of nationwide effect are similarly refuted by the uncontroverted facts that Subaru's and Kia's policies are limited to vehicles in Massachusetts, and neither Subaru nor Kia has had to withdraw from the Massachusetts market. ECF #262 ¶¶ 4&5; ECF #263-1 at 8-9.

Moreover, the Alliance's argument that OEMs will suffer irreparable harm if required to comply with the Data Access Law is further refuted by the amount of time the OEMs have had to develop mechanisms to comply with the law. *Cf. Respect Maine PAC*, 622 F.3d at 16 (in

determining weight to be accorded injunction claimants' allegation of harm, court may consider fact that the "'emergency' is largely one of their own making"). At trial, even the Alliance's own experts agreed that safe compliance with the Data Access Law was feasible, with some time to implement the changes. Tr.III:58 (Garrie); Tr.III.70-71, 75 (Bort). The Court warned the Alliance as early as January 2021 that "if their business planning is not including thinking about" the Data Access Law "coming into play at some point," they were "whistling by the graveyard on it." ECF #94 at 40. The Alliance's members—some of the largest corporations in the world—have now had approximately 30 months since the Data Access Law went into effect in December 2020 to develop mechanisms for compliance, and at least two OEMs have already made changes to comply. Those who have failed to seek to comply cannot rely on their own inaction to conjure up irreparable harm.

III. THE BALANCE OF THE EQUITIES FAVORS THE ATTORNEY GENERAL.

In balancing the equities, the Alliance's request for an injunction runs up against a serious problem: The Alliance's own longstanding pattern of inequitable conduct vis-à-vis complying with the Data Access Law.

A preliminary injunction, of course, "is an extraordinary and drastic remedy that is never awarded as of right." *Peoples Fed. Sav. Bank v. People's United Bank*, 672 F.3d 1, 8-9 (1st Cir. 2012). It is also a well-established principle of equity that "a court called upon to do equity should always consider whether the petitioning party has acted in bad faith or with unclean hands." *Texaco P.R., Inc. v. Dep't of Consumer Affairs*, 60 F.3d 867, 880 (1st Cir. 1995). This maxim of equity "closes the doors of a court of equity to one tainted with inequitableness or bad faith relative to the matter in which he seeks relief." *Precision Instrument Mfg. Co. v. Auto. Maint. Mach. Co.*, 324 U.S. 806, 814 (1945). Such a "taint" of inequitableness does not require criminal, or even legally actionable, conduct—rather, it is enough that the party who seeks equity

acts "[un]fairly." *Id*. at 814-15. And, "[w]here a suit in equity concerns the public interest . . . this doctrine assumes even wider and more significant proportions." *Id*. at 815.

Here, the Alliance has repeatedly acted unfairly toward the Data Access Law, a pattern that began to manifest itself even before the Law was enacted.

1. Before the initiative petition that would become the Data Access law was even drafted, the Alliance's members refused to work with the automotive aftermarket to develop and implement a method of providing independent repair facilities with secure access to repair and diagnostic-related telematics system data. ECF #191 ¶¶ 68-69, 71-74, 82 (Lowe Aff.).

2. Prior to the November 2020 election, GM's Kevin Tierney reviewed the then-proposed Data Access Law and—without discussing the law with any of GM's engineers, and without generating any notes, sketches, or documentation to memorialize this conclusion—unilaterally concluded that compliance was not achievable for GM. ECF #219 at 59-60.

3. Immediately after the November 2020 election, a group of GM engineers (who evidently hadn't gotten the memo) expressed their intention "in parallel to legal challenges . . . to revisit what a very-[minimal] type of technical solution could be and start planning for that." Tr. Exh. 512; *see also id*. (GM software engineer stating that his team would "start bouncing some ideas around on our side. Particularly how we might architect an interface to a third party portal. . . . [W]e'll start getting some thoughts together."). A few days later, however, when one of those engineers told Mr. Tierney that "he and his team would begin to understand . . . what minimally [GM] need[s] to do to meet the requirements of the law," Mr. Tierney deemed that engineer to lack the "full context" of the issue and arranged for that engineer to meet with GM's lawyers, after which the notion of exploring a technical solution disappeared into the ether. ECF #219 at 63-65.

4. Between the filing of this lawsuit in November 2020 and the time of trial in June 2021, neither GM nor Stellantis made any efforts to develop a technical means to comply with the Data Access Law. ECF #219 at 67, 112, 130. They failed to do so despite the Court's warning in January 2021 that "I really mean it about, if their business planning is not including thinking about [the Data Access Law] coming into play at some point, then they're whistling by the graveyard on it." ECF #94 at 39-40.

5. Between June 2021 and October of 2022, neither GM nor Stellantis made any efforts to develop a technical means to comply with the Data Access Law. ECF #296 ¶ 11 (Tierney Aff.); ECF #297 ¶ 4 (McKnight Aff.). To justify this failure, the Alliance reverts to its old strategy of interpreting the Data Access Law in extreme ways, but this does not excuse the OEM's utter dereliction of their responsibilities to comply with the law. Nor does it square with the trial testimony of the Alliance's own experts that, if the Data Access Law is interpreted as the Attorney General contends, technical compliance is "not far-fetched," not "exponentially burdensome," and "a lot more feasible." Tr. III:58, 70-71, 75; *see also* Tr. III:88-89 (Mr. Bort: "I think, yes, those systems exist; yes, we can adapt them. We are definitely in the long-term time frame. Reasonably, there are proven technologies, there are companies that could adapt this from other markets; and, again, we could put . . . do that.").

The Alliance also contends that "development of [the Law's] required mechanisms would take years, necessitating consensus from industry stakeholders other than OEMs; and, once they finally exist, OEMs would then need years to design, build, and test vehicles that use those mechanisms to ensure compliance with federal safety and emissions requirements." ECF #340 at 17. But, again, an "emergency" "of [the claimant's] own making" does not support the exercise of the Court's equitable authority. *Respect Maine PAC*, 622 F.3d at 16. Had the Alliance's members begun to pursue a technical means to comply with the Data Access Law when the need

to do so became apparent in November 2020—as some engineers at GM suggested at the time—there might well be no "emergency" at all. Such inequitable conduct on the part of the Alliance's members now bars the injunction they seek.

IV. THE PUBLIC INTEREST FAVORS ALLOWING A LAW OVERWHELMING APPROVED BY THE VOTERS TO TAKE EFFECT.

The Alliance asserts that an injunction is in the public interest, because allowing the Data Access Law to go into effect will result in unsafe vehicles on the roads. ECF #340 at 18. The Alliance also claims that the public interest is served by, in effect, allowing OEMs to continue to design, manufacture, and sell vehicles in the way they prefer. ECF #340 at 19.

As noted repeatedly in this memorandum, the trial evidence has demonstrated that an OEM can comply with the Data Access Law in a way that is safe and also complies with all applicable FMVSS, as well as the Clean Air Act and related regulations. But, at a more basic level, this Court need not attempt to divine the public interest on its own, because this is the unique case in which the public has already expressed its interest: As approximately 75% of Massachusetts voters affirmed in November 2020, Tr. Exh. 513 at 51-52, the public's interest is to give the Data Access Law full force and effect. It is remarkable that a corporate association of automobile manufacturers claims to know the public's interest better than the voters themselves do—and it exemplifies the Alliance's abject failure to justify the requested injunction.

CONCLUSION

For the foregoing reasons, the Alliance's request for injunctive relief should be denied. And, because the Alliance lacks standing and a cause of action, its preemption claims fail as a matter of law, and the evidence submitted at and after trial has confirmed that OEMs can comply with the Data Access Law without violating the MVSA or the CAA, this Court should enter judgment in favor of the Attorney General.

Respectfully submitted,

ANDREA JOY CAMPBELL
ATTORNEY GENERAL,

By her attorneys,

May 30, 2023

/s/ Eric Haskell
Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Christine Fimognari, BBO No. 703410
Assistant Attorneys General
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
(617) 963-2855
eric.haskell@mass.gov

CERTIFICATE OF SERVICE

I certify that a true copy of this document will be sent electronically by the ECF system to attorneys of record identified on the Notice of Electronic Filing.

May 30, 2023

/s/ Eric Haskell
Eric Haskell
Assistant Attorney General