IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

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

PLAINTIFF ALLIANCE FOR AUTOMOTIVE INNOVATION'S MEMORANDUM OF LAW IN SUPPORT OF ITS EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AND EXPEDITED HEARING

TABLE OF CONTENTS

PAGE

INTRODUCTION 1

BACKGROUND 3

ARGUMENT 4

I. The Court Should Issue A Temporary Restraining Order Precluding Enforcement Of The Data Access Law. 4

a. Auto Innovators Is Likely To Succeed On The Merits. 5

i. The Vehicle Safety Act Preempts The Data Access Law. 5

ii. The Clean Air Act Preempts The Data Access Law. 8

b. Auto Innovators' Members Will Suffer Irreparable Harm In The Absence Of An Injunction. 9

c. The Balance Of Equities Weighs Heavily In Auto Innovators' Favor. 12

d. A TRO Is In The Public Interest. 14

II. If The Court Requires Additional Time To Prepare Its Judgment, It Can Order Briefing On A Preliminary Injunction. 15

CONCLUSION 15

TABLE OF AUTHORITIES

Page(s)

Cases

Axia NetMedia Corp. v. Mass. Tech. Park Corp.,
251 F. Supp. 3d 301 (D. Mass 2017) 4, 10

Bruns v. Mayhew,
750 F.3d 61 (1st Cir. 2014) 4

Crosby v. Nat'l Foreign Trade Council,
530 U.S. 363 (2000) 5

Freightliner Corp. v. Myrick,
514 U.S. 280 (1995) 5

Home Market Foods, Inc. v. Lubow,
No. 1:20-cv-12180-DPW (D. Mass. Dec. 16, 2020) 5

Rio Grande Cmty. Health Ctr., Inc. v. Rullan,
397 F.3d 56 (1st Cir. 2005) 12

Ross-Simons of Warwick, Inc. v. Baccarat, Inc.,
102 F.3d 12 (1st Cir. 1996) 10

Vaquería Tres Monjitas, Inc. v. Irizarry,
587 F.3d 464 (1st Cir. 2009) 5

Zaya v. Adducci,
2020 WL 2079121 (E.D. Mich. Apr. 30, 2020) 14

Zogenix, Inc. v. Patrick,
2014 WL 1454696 (D. Mass. Apr. 15, 2014) 13

Statutes

42 U.S.C. § 7401 *et seq.* 1, 9

42 U.S.C. § 7521 9

42 U.S.C. § 7522 9

42 U.S.C. § 7543 9

42 U.S.C. § 7547 9

49 U.S.C. § 30101 *et seq.* 1, 6

49 U.S.C. § 30111 6

49 U.S.C. § 30118 6

49 U.S.C. § 30119 6

49 U.S.C. § 30120 6

49 U.S.C. § 30122 ..... 6, 8

Other Authorities

42 C.F.R. § 86.1845-04 9

49 C.F.R. § 571.124 6

49 C.F.R. § 571.126 6

49 C.F.R. § 571.135 6

49 C.F.R. § 571.208 6

Mass. Gen. L. ch. 93K, § 1 7

Mass. Gen. L. ch. 93K, § 2 ..... 7, 8, 11, 12

INTRODUCTION

Though the Court has not yet issued its ruling or judgment in this matter, the Attorney General has informed the Court and the parties that she intends to terminate her non-enforcement stipulation effective June 1, 2023. *See* ECF No. 330. The Attorney General also has informed Auto Innovator's counsel that she intends to issue the "telematics system notice" contemplated by the Data Access Law without soliciting any public comment on that notice, presumably on or shortly after June 1. Thus, as the Court contemplated (*see* July 21, 2021 Trial Tr. 3:24-4:5), Plaintiff Alliance for Automotive Innovation ("Auto Innovators") has no choice but to seek a temporary restraining order barring enforcement of the Data Access Law until the Court renders a judgment in this action, or until the Court can issue a preliminary injunction granting such relief.

A TRO is unequivocally warranted here. As set forth in Auto Innovators' post-trial briefing, the trial record establishes that Auto Innovators should prevail on its preemption claims, and therefore has more than a reasonable likelihood of success on the merits. As Auto Innovators established at trial, federal law preempts the Data Access Law because it requires original equipment manufacturers ("OEMs") to eliminate existing cybersecurity and emissions controls, which directly conflicts with the requirements, purposes, and objectives of the federal National Traffic and Motor Vehicle Safety Act (the "Vehicle Safety Act"), 49 U.S.C. § 30101, *et seq.*, and the Clean Air Act, 42 U.S.C. § 7401, *et seq*. Compliance with the Data Access Law is mutually exclusive with compliance with these federal Acts.

Auto Innovators also has demonstrated that its members will suffer irreparable harm absent a TRO. Even if an OEM was somehow willing to overlook its federal safety obligations, as established at trial, any attempt to comply with the Data Access Law would require an OEM to remove essential cybersecurity protections from their vehicles. Once vehicles without those protections are sold in the Commonwealth, those protections cannot be reinstalled in those

vehicles if the law is later vacated. Similarly, OEMs that try to avoid the need to comply with part of the Data Access Law by disabling telematics (as the Attorney General has proposed) would remove important safety, entertainment, and other features that consumers rely upon every day—and thereby harm consumers and incur irreparable reputational harm that again cannot be remedied if the law is later vacated. Other OEMs may be forced to withdraw from the Massachusetts market altogether, destroying their relationships with their dealers and causing incalculable harm to their brands, goodwill and reputation. Further, the Attorney General's plan to issue the "telematics system notice" without seeking any public comment or input on that notice may well misinform prospective vehicle owners and thereby harm OEMs.

Moreover, as the United States recognized in its Statement of Interest filed in this action (*see* ECF No. 202 at 6-7, 8-9), the required introduction of untested "open access" vehicle systems that the Data Access Law requires will create unwarranted dangers for the driving public. Disabling vehicles' telematics units to avoid compliance would harm Massachusetts drivers who paid for, and rely upon, the many vehicle functions that telematics provides. And these consequences would occur even though OEMs have already complied with Massachusetts' preexisting right-to-repair law, which *already* gives vehicle owners the full ability to have their vehicles repaired by any independent service provider of their choosing. The balance of the equities and the public interest therefore weigh heavily in favor of a TRO so Massachusetts' drivers are not exposed to safety risk and deprived of important features in their vehicles until this case can finally be resolved.

Thus, the Court should grant a TRO to prevent enforcement of the Data Access Law until the Court can render a judgment voiding that law or at least until the Court can consider a preliminary injunction requesting such relief.[1]

[1] In the alternative, if the Court were to issue a judgment denying Auto Innovators' preemption claims, Auto Innovators will at that time seek equitable relief pending appeal; but even in that event, a TRO would be warranted until Auto Innovators has the ability to seek such a stay.

BACKGROUND

The Data Access Law passed by ballot initiative on November 3, 2020. Auto Innovators filed this action shortly thereafter, on November 20, 2020, and it moved for a preliminary injunction on December 1, 2020. ECF Nos. 1, 26–48. Instead of ruling on Auto Innovators' preliminary injunction motion, the Court determined that it should rule based on a full evidentiary record, developed after discovery and a trial. At the Court's request, the Attorney General agreed not to enforce the Data Access Law until after the Court ruled on Auto Innovators' claim following a bench trial. *See, e.g.*, ECF Nos. 50, 51. Based on these representations and stipulation, Auto Innovators conditionally withdrew its motion for a preliminary injunction on December 7, 2020. *See* ECF No. 51.

Following expedited fact and expert discovery, the Court held a bench trial spanning June and July 2021. ECF Nos. 205, 207-08, 222, 237. At the conclusion of the trial, the Court requested that the Attorney General extend her non-enforcement stipulation until August 20, 2021 to give the Court time to prepare its findings of fact and conclusions of law. July 21, 2021 Tr. 3:24-4:7. The Court noted that if the Attorney General declined to extend her stipulation, it would "take whatever steps I need to take, including a temporary restraining order with respect to it." *Id.* Ultimately, the Attorney General consented to extend her stipulation at the Court's request. *See* ECF No. 244, 273.

After trial, several additional developments occurred that delayed the Court's ability to rule in this action. For instance, on October 22, 2021, the Attorney General moved to reopen the evidence, and new evidence was submitted in January 2022. ECF Nos. 262-64. In September 2022, the Court observed that there had been new developments that had affected the Court's timing of its decision, including new information about the "dangers of cybersecurity," prospective FTC rulemaking on private data collection, and actions by the California Air Resources Board. *See* Sep. 1, 2022 Tr. 5:10-6:4. In November 2022, Auto

Innovators requested additional post-trial discovery from the Auto Care Association ("ACA") regarding a proposed ballot initiative in Maine. ECF No. 305. On January 5, 2023, the Court allowed Auto Innovators to take limited discovery on that issue. ECF No. 318. That discovery concluded in March 2023, and the parties briefed the impact of that discovery in April 2023. *See* ECF Nos. 335-37.

Despite the post-trial activity, the Attorney General filed a notice of intent to terminate her non-enforcement stipulation on March 7, 2023, with an effective date of June 1, 2023. ECF No. 330. On March 31, 2023, the Court entered an order dismissing certain of Auto Innovators' claims, but denying the Attorney General's motion to dismiss Auto Innovators' claims for declaratory judgment that the Vehicle Safety Act and the Clean Air Act preempt the Data Access Law. *See* ECF No. 334. The Court explained that it would develop its reasoning "in the Memorandum to be issued regarding the Findings and Conclusions" that will "provid[e] the basis for Final Judgment in this case." *Id.* To date, however, the Court has not issued a final judgment in this action.

ARGUMENT

I. The Court Should Issue A Temporary Restraining Order Precluding Enforcement Of The Data Access Law.

"In deciding a motion for a temporary restraining order, 'a district court weighs four factors: (1) the plaintiff's likelihood of success on the merits; (2) the potential for irreparable harm in the absence of an injunction; (3) whether issuing an injunction will burden the defendants less than denying an injunction would burden the plaintiffs; and (4) the effect, if any, on the public interest.'" *Axia NetMedia Corp. v. Mass. Tech. Park Corp.*, 251 F. Supp. 3d 301, 305-06 (D. Mass 2017) (citation omitted). "[T]he first two factors, likelihood of success and of irreparable harm, [are] 'the most important' in the calculus." *Bruns v. Mayhew*, 750 F.3d 61, 65 (1st Cir. 2014) (citation omitted). "[T]he measure of irreparable harm is not a rigid one; it has been referred to as a sliding scale, working in conjunction with a moving party's

likelihood of success on the merits." *Vaquería Tres Monjitas, Inc. v. Irizarry*, 587 F.3d 464, 485 (1st Cir. 2009)). Here, each of the four factors weighs heavily in favor of granting a TRO in this action.

a. Auto Innovators Is Likely To Succeed On The Merits.

The first factor is Auto Innovators' likelihood of success on the merits of its remaining claims for declaratory relief with respect to the Vehicle Safety Act and Clean Air Act. For the reasons detailed at trial and in Auto Innovators' post-trial findings of fact and conclusions of law (*see* ECF No. 233) and as summarized below, both the Vehicle Safety Act and the Clean Air Act conflict with and preempt the Data Access Law.

It is a "fundamental principle of the Constitution" that "Congress has the power to preempt state law." *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372 (2000) (citing U.S. Const. art. VI, cl. 2). Congress may preempt state law when "state law is in actual conflict with federal law." *Freightliner Corp. v. Myrick*, 514 U.S. 280, 287 (1995) (citation omitted). Conflict preemption exists "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." *Id.* (internal quotations omitted).

Here, it remains clear that the Data Access Law is invalid under well-established conflict-preemption principles. Compliance with the Data Access Law would require OEMs to abandon existing cybersecurity and emissions controls that protect core vehicle functions—directly controverting the requirements, purposes, and objectives of the Vehicle Safety Act and the Clean Air Act.

i. The Vehicle Safety Act Preempts The Data Access Law.

Congress passed the Vehicle Safety Act to "reduce traffic accidents and deaths and injuries resulting from traffic accidents." 49 U.S.C. § 30101. To achieve this purpose, the Vehicle Safety Act empowers NHTSA to issue Federal Motor Vehicle Safety Standards

("FMVSSs") and to issue recalls that address and remediate safety-related defects arising in vehicles. 49 U.S.C. §§ 30111, 30118-20. Further, that 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 applicable motor vehicle safety standard prescribed under this chapter." 49 U.S.C. § 30122.

Among the "devices" and "elements of design" that manufacturers install in motor vehicles "in compliance with an applicable motor vehicle safety standard" (*id.*) are acceleration, braking, steering, and air bag systems. NHTSA regulates extensively in these areas, including by issuing applicable FMVSSs. *See* 49 C.F.R. § 571.124 (acceleration control devices); *id.* § 571.126 (electronic stability control, including steering and anti-lock braking systems); *id.* § 571.135 (light-vehicle braking systems); *id.* § 571.208 (occupant crash protection, including air bags). And Auto Innovators' members have installed a variety of cybersecurity protections around regulated vehicle functions to help prevent threat actors (or others) from taking control of these and other core vehicle functions and, ultimately, the vehicle itself. *See* ECF No. 233 (Pl. Post-Tr. Prop. Findings of Fact ("PFOF")) ¶¶ 23-61, 65-78. These cybersecurity protections are key "part[s]" of the "device or element of design" of vehicles, which allow them to comply with federal motor vehicle standards. 49 U.S.C. § 30122(b).

Yet the Data Access Law requires motor vehicle manufacturers to remove cybersecurity protections. *First*, Section 2 of the Data Access Law imposes two alternative requirements: OEMs must "standardize[]" access to their on-board diagnostic systems and make them accessible without "any authorization by the manufacturer, directly or indirectly." Mass. Gen. L. ch. 93K, § 2(d)(1). Or they must implement in their vehicles 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.* It was undisputed at trial that (a) 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," and (b) there is no "entity unaffiliated with a manufacturer" that could run a standardized authorization system. *See*, *e.g.*, June 15, 2021 Tr. 13:13-15, 24:24-25-15 (Lowe); *id.* 96:18-97:3 (Potter); *see also id.* 118:11-13 (Attorney General expert confirming there is "no immediate way to comply with section 2 of the Data Access Law"). And the interests behind the Data Access Law have made no efforts since the trial to create this critical independent third party entity. *See* ECF No. 336-7 (Lowe Dep.) 44:14-21, 96:2-6 (testifying that independent entity required by Section 2 still did not exist as of March 2023). As a result, to even attempt to comply with Section 2, OEMs would need to "standardize[]" their OBD systems and remove any form of "authorization"—and thereby abandon their existing cybersecurity controls. *E.g.*, June 14, 2021 Tr. 70:6-14, 71:18-72:3, 73:14-75:11 (Tierney); ECF No. 199 (Chernoby Tr. Aff.) ¶ 65; ECF No. 197 (Tierney Tr. Aff.) ¶¶ 13, 90.

Second, Section 3 of the Data Access Law requires manufacturers to create an "inter-operable, standardized, and open access" "platform" beginning in model year 2022 vehicles. Mass. Gen. L. ch. 93K, § 2(f). That platform also must be "[d]irectly accessible by the owner of the vehicle through a mobile-based application" and "[c]apable of securely communicating all mechanical data emanating directly from the motor vehicle via 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). Further, 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.* § 2(f).

Every expert at trial agreed that OEMs could *not* provide the inter-operable, standardized, and open access platform that Section 3 requires (*see* June 16, 2021 Tr. 41:21, 42:1-10 and that no "mobile-based application" currently exists that could be used to comply with the law, *see, e.g.*, June 15, 2021 Tr. 95:21-96:17 (Potter); *id.* at 126:13-15 (Smith). And as with Section 2, any attempt to comply with Section 3's "open access" regime for broadly-defined "mechanical data" would require OEMs to remove or disable important cybersecurity controls that protect safety-critical vehicle functions. *See, e.g.*, June 14, 2021 Tr. 72:4-17 (Tierney); ECF No. 197 (Tierney Tr. Aff.) ¶¶ 90, 99; June 14, 2021 Tr. 126:20-127:10 (Chernoby); ECF No. 201 (Garrie Tr. Aff. ¶ 90).

Removing and degrading motor vehicles' cybersecurity protections would put motor vehicle manufacturers out of compliance with federal law. Doing so would frustrate the purposes and objectives of the Vehicle 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* ECF No. 233 (Pl. Post-Tr. Prop. Conclusions of Law ("PCOL")) ¶¶ 100-14. Similarly, removing or degrading OEMs' cybersecurity protections would violate the Safety Act's prohibition on manufacturers "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); *see also* Pl. PCOL ¶¶ 115-25.

In short, because the Vehicle Safety Act preempts the Data Access Law, Auto Innovators has demonstrated a likelihood of success on its first claim for declaratory relief.

ii. The Clean Air Act Preempts The Data Access Law.

Likewise, through the Clean Air Act, Congress has established a comprehensive statutory scheme to control air pollution from all sources throughout the United States. 42 U.S.C. §§ 7401, *et seq.* With certain limited exceptions not applicable here, that Act vests the

federal government, acting through EPA, with exclusive authority to regulate mobile sources, including from motor vehicles. 42 U.S.C. §§ 7521, 7543, 7547. The Act imposes stringent vehicle emissions requirements on manufacturers, including by requiring in-use verification testing or post-sale testing. *Id.* § 7521(d), 7541(a)(1); 42 C.F.R. § 86.1845-04. And, like the Vehicle Safety Act, the Clean Air Act prohibits manufacturers and other persons from removing or "render[ing] inoperative" any "device or element of design installed on or in a motor vehicle or motor vehicle engine." 42 U.S.C. § 7522(a)(3)(A).

Here, the cybersecurity protections that manufacturers have installed around vehicles' engine control modules are considered "element[s] of design." *Id.* Manufacturers are precluded by the Clean Air Act from now rendering those inoperative to comply with the Data Access Law. *E.g.*, ECF No. 197 (Tierney Tr. Aff.) ¶¶ 82, 90, 94, 97, 100-01; ECF No. 199 (Chernoby Tr. Aff.) ¶¶ 13, 26, 59, 61, 64-69, 80-82. And because compliance with the Data Access Law would require removing those cybersecurity protections, vehicle owners and third parties could more easily access vehicles' engine control modules to disable emissions control systems via aftermarket software designed for that purpose. ECF No. 233 (PFOF) ¶¶ 92-96. Because OEMs cannot comply with both the Clean Air Act and the Data Access Law, there is a clear conflict between federal and state law and the state law must yield. U.S. Const. art. VI. Accordingly, the Data Access Law is preempted by the Clean Air Act and thus void and unenforceable—and Auto Innovators has demonstrated a likelihood of success on its second claim for declaratory relief, as well.

b. Auto Innovators' Members Will Suffer Irreparable Harm In The Absence Of An Injunction.

The second factor for the Court to consider is the likelihood that Auto Innovators' members will suffer "irreparable harm in the absence of an injunction." *Axia*, 251 F. Supp. 3d at 305. To demonstrate irreparable harm, a plaintiff need only show that it will "suffer[] a substantial injury that is not accurately measurable or adequately compensable by monetary

damages." *Ross-Simons of Warwick, Inc. v. Baccarat, Inc.*, 102 F.3d 12, 18-19 (1st Cir. 1996). Auto Innovators easily meets this burden: unless the Court issues a TRO, enforcement of the Data Access Law will inflict immediate and irreparable injuries that damages alone cannot remedy.

With the Attorney General set to begin enforcement of the Data Access Law, Auto Innovators' members find themselves in an impossible position. As explained, OEMs have existing federal obligations that conflict with the Data Access Law's requirements. OEMs' vehicle systems are already a prime target for cyberattack (*see* ECF No. 201 ¶¶ 11-18; ECF No. 200 ¶¶ 19-24), and if Auto Innovators' members even attempted to comply with the Data Access Law, they would have to alter their vehicles in a manner that would increase the cybersecurity risks to safety- and emissions-critical vehicle systems. *See, e.g.*, June 14, 2021 Tr. 200:20-201:8 (Bort) ("[I]nherently, compliance requires the abrogation of the protections that have been built into them that have just been layered and built up over time."); *id.* 70:6-21, 71:18-72:3, 73:14-22 (Tierney) (explaining how compliance with the Data Access law would require removal of critical GM functions); ECF No. 202 (U.S. Statement of Interest) at 8 ("the Data Law requires motor vehicle manufacturers to take actions that potentially pose serious cybersecurity risks by opening uncontrolled access to vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking, which are designed in a manner that expect (and require) authenticated privileged access rights in existing implementations").[2] Thus, attempted compliance with the Data Access Law would subject OEMs to federal scrutiny, enforcement, and penalties, as well as enormous potential recall and

[2] *See also, e.g.*, June 15, 2021 Tr. 113:3-21 (Smith) (confirming that "the Data Access Law would require OEMs to make changes to the cybersecurity they have on their vehicles today"; that "altering cyber protections that exist on a vehicle could make them more vulnerable to cyber attacks"; that "with the correct access, hackers can take over core functionality of a vehicle"; and that hackers could "thwart safety systems or install malware on a vehicle," among other possibilities); ECF No. 201 (Garrie Tr. Aff.) ¶ 64 ("To comply with the Data [Access] Law, OEMs would have to remove or alter critical cybersecurity controls, which would substantially increase the safety risks of using their vehicles").

repair costs if compliance with the Data Access Law renders vehicles' safety and emissions systems defective. Yet if they continue to follow federal law, OEMs will be in violation of the Data Access Law, which the Attorney General now promises to enforce under threat of significant penalties. Further, even if any OEMs were willing to overlook their federal safety obligations and attempt to comply with the Data Access Law, once vehicles without those protections are sold, the OEMs could not replace vehicles' cybersecurity protections if the law is later vacated.

Moreover, any OEMs that follow the Attorney General's proposal and disable telematics in their vehicles to avoid penalties for violating Section 3 (ECF No. 233 (PFOF) ¶ 126)) would be removing safety features such as firmware-over-the-air (FOTA) updates. ECF No. 200 (Bort Tr. Aff.) ¶ 96; ECF No. 201 (Garrie Tr. Aff.) ¶ 100; ECF No. 199 (Chernoby Tr. Aff.) ¶ 83; ECF No. 197 (Tierney Tr. Aff.) ¶ 112; June 15, 2021 Tr. 118:14-21 (Smith). NHTSA specifically encourages FOTA updates to facilitate vehicle safety features, such as emergency crash notifications. ECF No. 200 (Bort) ¶ 96; ECF No. 201 (Garrie) ¶ 100. And turning off telematics would also impact non-safety features that drivers bought their vehicles expecting to be able to use every day, such as GPS, entertainment systems, and remote-start functionality. *See, e.g.*, ECF No. 201 (Garrie) ¶ 34; ECF No. 197 (Tierney) ¶ 36. Worse, any mechanism for potential disabling telematics units likely could not be cabined just to Massachusetts residents—so the harm to vehicle owners could be felt nationwide. *See* ECF No. 197 (Tierney) ¶ 111; ECF No. 201 (Garrie) ¶ 99. Other OEMs may need to withdraw from the Massachusetts market altogether to avoid the conflicting legal regimes that the Data Access Law imposes.

Finally, when meeting and conferring with Auto Innovators' counsel on this Motion, the Attorney General disclosed that she plans to issue the "telematics system notice" contemplated by the Data Access Law (*see* Mass. Gen. L. ch. 93K, § 2(g)) without seeking any public comment. Because the Court has not yet issued its ruling interpreting the law, and

because OEMs have had no opportunity to comment on that notice, the notice may well be inaccurate. For example, the Data Access Law states that the notice should include information on "an owner's right to authorize an independent repair facility to access the vehicle's mechanical data" (*id.*); however, according to the law, that access must be "standardized and not require any authorization by the manufacturer . . . unless the authorization system . . . is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer." *Id.* § 2(d)(1). As has been well-established in the record, there is no such standardized system administered by an unaffiliated entity, and it would be misleading to consumers and harmful to OEMs for the forthcoming notice to suggest otherwise. Therefore, if vehicle dealers in Massachusetts are forced to provide that notice to their customers (*id.* § 2(h)), their customers may be misinformed and OEMs will be harmed.

Thus, the Attorney General's immediate enforcement of that law would impair OEMs' relationships with vehicle owners throughout the United States, disrupt or destroy its dealer relationships, and cause untold reputational damage to OEMs. These imminent risks of harm are classic "irreparable injuries" because they "cannot adequately be compensated for either by a later-issued permanent injunction, after a full adjudication on the merits, or by a later-issued damages remedy." *Rio Grande Cmty. Health Ctr., Inc. v. Rullan*, 397 F.3d 56, 76 (1st Cir. 2005).

c. The Balance Of Equities Weighs Heavily In Auto Innovators' Favor.

The third TRO factor—balancing the equities—also weighs heavily in favor of Auto Innovators. Auto Innovators' members will suffer immediate irreparable harm if the Attorney General begins enforcing the Data Access Law on June 1, while neither the Attorney General nor the citizens of Massachusetts will suffer any harm from the continued stay of enforcement of a law that is impossible for OEMs to comply with in any event.

As explained, motor vehicle manufacturers' only option even to attempt to comply with the law—where critical prerequisites do not even exist—is to strip their vehicles of cybersecurity

protections. Doing so risks major penalties under the Vehicle Safety Act; they could be forced to recall entire fleets of vehicles. Moreover, the resulting cybersecurity risks will jeopardize OEMs' reputations, imposing a potentially incalculable loss. All it would take is one well-timed hack to undo decades of an OEM's efforts to build its reputation as a manufacturer of safe and reliable vehicles. The threat of that sort of reputational harm is a classic basis for equitable relief. *See, e.g.*, *Zogenix, Inc. v. Patrick*, 2014 WL 1454696, at *2 (D. Mass. Apr. 15, 2014) (balance of equities weighed in a drug company's favor where company would suffer from reputational injury from defendant's publicized ban of the drug, and that ban was likely preempted by the FDA's authority to issue the drug as safe for use).

The inequity to Auto Innovators' members is particularly acute given that, no matter what they do, they still cannot fully comply with the Data Access Law. Again, though Section 2 of the law contemplates a "standardized" "authorization system for access to vehicle networks and their on-board diagnostic systems," as well as an "entity unaffiliated with a manufacturer" that could run that authorization system in place of the OEMs themselves, the Attorney General's own witnesses agree that neither currently exists. *See, e.g.*, June 15, 2021 Tr. 13:13-15, 24:24-25-15 (Lowe); *id.* 96:18-97:3 (Potter); ECF No. 336-7 (Lowe Dep.) 44:14-21, 96:2-6. Nor can the OEMs create and fund such an entity, as then it would not be unaffiliated with them. Likewise, Section 3 contemplates an inter-operable, standardized, open access platform that every expert agreed does not exist. *E.g.*, June 16 Tr. 41:21, 42:1-10. The Data Access Law's requirements are aspirational at best. The development of its 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. *See* ECF No. 296 (Tierney Decl.) ¶¶ 14, 17, 26, 35; ECF No. 297 (McKnight Decl.) ¶¶ 6-7.

In contrast to this harm, the purported beneficiaries of the Data Access Law—the citizens of Massachusetts—will not suffer any harm from the proposed TRO. A TRO would simply keep in place the status quo: temporary non-enforcement while this Court crafts its decision based on the evidence presented at trial. Moreover, the public-facing purpose of the Data Access Law is to provide Massachusetts consumers with the ability to have their vehicles repaired at the independent repair shop of their choice. Pre-existing Massachusetts law *already requires* OEMs to provide independent technicians with access to diagnostic and repair information and the ability to use the same diagnostic tools that dealers can—such that Massachusetts vehicle owners already have the ability to take their vehicles to any independent service provider of their choice. ECF No. 233 (PFOF) ¶¶ 99-101; *see also* ECF No. 296 (Tierney Decl.) ¶¶ 5-10. Regardless, any additional short-term delay in the enforcement of the Data Access Law pending resolution of this action cannot possibly outweigh the tremendous inequity that immediate enforcement would impose on Auto Innovators' members, particularly where the drafters of the Data Access Law purposefully crafted it in a way that immediate compliance would be impossible so they would have a "bargaining chip" in negotiations with the OEMs. June 15, 2021 Tr. 51:9-53:3; *see also* Ex. 62 at AAI-ACA-0038565-68 (noting that OEMs are unlikely to be able to meet the deadlines in the law but opposing extending the timeline).

d. A TRO Is In The Public Interest.

The fourth and final factor is whether that TRO is in the public interest. Here, that undoubtedly is the case. It is axiomatic that "[p]rotecting public health and safety is in the public interest." *Zaya v. Adducci*, 2020 WL 2079121, at *8 (E.D. Mich. Apr. 30, 2020). Enjoining the Data Access Law until the Court renders a judgment will serve the public interest by ensuring that OEMs do not have to abandon safe and secure vehicle systems for ones that NHTSA has recognized as posing substantial consumer safety risks. *See* ECF No. 202 (U.S. Statement of Interest) at 8, 9, Ex. 1 at 2-4.

Likewise, as noted, the issuance of a TRO would prevent the need for OEMs to disable the telematics units in their vehicles, or to exit the Massachusetts market altogether. Drivers therefore would continue to benefit from consumer choice and from the safety and non-safety features that telematics units provide.

II. If The Court Requires Additional Time To Prepare Its Judgment, It Can Order Briefing On A Preliminary Injunction.

Auto Innovators contends that the existing record in this case—including the testimony and other evidence from trial, as well as the parties' post-trial evidence and submissions—establishes that it should prevail on its claims and that the Court should permanently enjoin enforcement of the Data Access Law. Pending the issuance of such a judgment, the Court may enter a temporary restraining order preventing the Attorney General's immediate enforcement of the Data Access Law and, if it deems appropriate, order briefing on a motion for preliminary injunction. *See, e.g.*, Order, *Home Market Foods, Inc. v. Lubow*, No. 1:20-cv-12180-DPW, Dkt No. 11 (D. Mass. Dec. 16, 2020) (extending TRO "to permit an orderly briefing schedule for the requested preliminary injunction"). This would have the effect of maintaining the status quo while the Court prepares to issue its decision on the Court's desired timeline.

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court (a) enter a TRO, in the form attached to Plaintiff's Motion as Exhibit A, barring the Data Access Law from taking effect on June 1, 2023; and (b) provide for additional briefing on a preliminary injunction.

Dated: May 25, 2023

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Laurence A. Schoen
Laurence A. Schoen, BBO # 633002
Elissa Flynn-Poppey, BBO# 647189
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@mayerbrown.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 the above and foregoing was filed electronically through the Court's electronic filing system and that notice for this filing will be sent to all counsel of record in this matter by operation of the Court's ECF system and to non-registered users by first class mail.

Dated: May 25, 2023

/s/ Laurence A. Schoen
Laurence A. Schoen