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**

PLAINTIFF'S TRIAL BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Federal Constitutional Provisions, Statutes, and Regulations

State Statutes

Other Authorities

INTRODUCTION

Federal law preempts the ballot initiative now codified at Mass. Gen. L. ch. 93K, §§ 1, 2(d)(1), 2(f)-(h), 6 (the "Data Law"), because it unconstitutionally conflicts with the requirements, purposes, and objectives of the National Traffic and Motor Vehicle Safety Act (the "Safety Act"), 49 U.S.C. § 30101, *et seq.*, and the Clean Air Act, 42 U.S.C. § 7401, *et seq*. Those laws, and the regulations and enforcement regime implementing them, aim to protect safety- and emissions-critical vehicle functions from intentional (or even unintentional) manipulation. The Data Law impermissibly requires vehicle manufacturers to remove or seriously degrade cybersecurity controls that they have implemented as elements of design aimed to achieve those ends. Accordingly, the Data Law unconstitutionally conflicts with federal law, and the Court should strike it down in its entirety.

A cyberattack on even a single motor vehicle carries enormous public safety risk. If a vehicle is infected by malware or taken over by a remote operator bent on harm, that vehicle, operating at highway speeds, would present a danger to its driver, its passengers, others on the road, and its surroundings. That risk, and the consequences of any successful cyberattack, is magnified dramatically if *all* vehicles on Massachusetts roads suddenly became potential means of attack. Protecting vehicles from that cybersecurity risk is an extremely challenging undertaking: Malicious actors, some sponsored by hostile foreign governments, have the motivation, resources, and tools available to access safety-critical systems.[1]

[1] These sorts of cyberattacks are increasingly commonplace. *See, e.g.*, C. Goldbaum & W.K. Rashbaum, *The M.T.A. Is Breached by Hackers as Cyberattacks Surge*, N.Y. Times (Jun. 2, 2021), https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html (hackers penetrate network vulnerabilities in N.Y. subway system); J. Creswell et al., *Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business*, N.Y. Times (Jun. 1, 2021), https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html (recent cyberattack shut down a large portion of the U.S. meat-processing industry, seeking a ransom); C. Eaton & D. Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall St. J. (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 (ransomware attack of pipeline); D. Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the Solar Winds Attack*, NPR

If allowed to take effect, the Data Law would make serious cyberattacks much more likely and deadly than the attacks on pipelines and meat processers currently in the news. To comply, manufacturers must remove or seriously degrade existing cybersecurity controls that help to protect electronic vehicle systems—exposing safety-critical functions to hacks from hostile actors anywhere in the world.

The backers of the Data Law proposed it [redacted] Nonetheless, they pressed forward, [redacted], and focused on the millions of dollars they thought the law would let them take from Massachusetts citizens and all the money they could make from vehicle data.[2]

Fortunately, the Data Law cannot take effect, because it is preempted by federal law. It requires manufacturers to eliminate or significantly degrade cybersecurity controls that protect safety- and emissions-critical vehicle functions (and thereby ensure the safe operation of vehicles within prescribed emissions limits). That state-law obligation conflicts with the requirements, purposes, and objectives of the Safety Act and the Clean Air Act and is therefore unconstitutional.

(Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (Russian state-sponsored actor slipped malicious code into software, compromising data from Microsoft, Intel, and Cisco, as well as several government agencies); K. Benner, *U.S. Charges Chinese Military Officers in 2017 Equifax Hacking*, N.Y. Times (Feb. 10, 2020, updated May 7, 2020), https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html (hackers steal trade secrets and personal data of 145 million Americans).

[2] The Auto Care Association ("ACA") had been after vehicle telematics data for years, not for vehicle repair but as a "marketing opportunity," "seeking to leverage [it] to develop and market innovative services to consumers." Pl.'s Exhibit AO (AAI-ACA-0001657-58). The ACA planned to create and run the independent third party credentialing authority the Data Law demands. [redacted] An ACA consultant calculated that the ACA itself stood to make almost $800 million in the next ten years just from running the credentialing authority. Deposition Transcript of Taylor Mitchell ("Mitchell Tr."), at 83:17-22; [redacted] The ACA contemplated making that money—and sharing tens of millions more with the Massachusetts government itself—by charging fees to every vehicle owner in the Commonwealth. Mitchell Tr. at 126:14-127:8, 141:14-20. [redacted]

ARGUMENT

I. The Data Law Is Preempted by Federal Law.

The Data Law, like all state laws, must fall in the face of conflicting federal 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). 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." *Freightliner Corp. v. Myrick*, 514 U.S. 280, 287 (1995) (internal quotations omitted).[3] Because compliance with the Data Law would require manufacturers to violate the requirements, purposes, and objectives of the Safety Act and the Clean Air Act, the Law is preempted. CoL ¶¶ 44-79.

A. The Data Law Would Require Manufacturers to Remove or Significantly Degrade Existing Cybersecurity Controls.

Manufacturers use robust cybersecurity controls to help to ensure the safety of their vehicles and vehicle systems, and to protect systems regulating exhaust emissions against (illegal) tampering to boost vehicle performance. FoF ¶¶ 18-19, 53, 56, 59, 62, 77-78. As discussed below, the Data Law would require that those controls be eliminated in whole or substantial part.

1. Today's vehicles are effectively complex computers on wheels, comprising a variety of networks, electronic control units ("ECUs"), and hundreds of millions of lines of software code. FoF ¶ 5. An ECU can control a function such as steering or braking. *Id.* ¶ 6. Individual ECUs are connected through a vehicle Controller Area Network ("CAN") bus. *Id.* ¶ 5. These electronic systems have enabled manufacturers to create safer and more fuel-efficient vehicles. At the same time, as with any connected electronic systems, they raise safety and security challenges. *Id.* ¶ 16.

[3] *See also* Plaintiff's Proposed Findings of Fact and Conclusions of Law ("FoF"/"CoL") ¶¶ 35-42.

Manufacturers' cybersecurity measures control and protect the flow of messages in vehicle systems to prevent cybersecurity threats. *E.g.*, FoF ¶¶ 18-19. In doing so, manufacturers ensure that only authorized persons can access (or alter) vehicle systems and data that control safety- and emissions-critical functions. *Id.* at ¶¶ 17-44, 89. Among these cybersecurity controls are several important design elements that manufacturers install in vehicles to protect safety- and emissions-critical functions: secured gateways, *id.* at ¶¶ 9, 19, 28, 29, 34, 37, challenge and response protocols, *id.* at ¶¶ 9, 19-23; and authentication controls, *id.* at ¶¶ 9, 19, 26, 27.

Secured gateways. Secured gateways ensure the physical and logical isolation (or segmentation) of messages traveling between individual ECUs as key design elements to protect safety- and emissions-critical functions. FoF ¶¶ 19, 28-29, 34, 37, 53, 56, 59, 62, 78. Physical isolation refers to using separate processors for different vehicle functions. *Id.* at ¶ 28. Logical isolation refers to preventing direct communication between different vehicle features. *Id.* Together, this segmentation makes it more difficult for potentially malicious messages to travel between different groups of ECUs—like, for instance, preventing messages added through unauthorized access to a vehicle's telematics system from traveling to the vehicle's electronic brake control module. *Id.* at ¶¶ 28-29. Firewalls within the secured gateway help to contain any security breach by limiting it from reaching all of a vehicles' ECUs—particularly safety- and emissions-critical ECUs. *Id.* at ¶ 32.

Challenge and response protocols. When an actor requests access to protected vehicle data or functions, the vehicle issues a "challenge." FoF ¶ 20. The actor must give the correct "response" to unlock the requested data or function. *Id.* These protocols help ensure that repair technicians (whether from a dealership or an independent repair shop) do not write data to the vehicle that could compromise its software or firmware when accessing a limited subset of vehicle

diagnostic data through a vehicle's SAE J2534-compliant port. *Id.* at ¶ 21. Technicians connect to this port with a physical tool—often called a "scan tool." *Id.* Challenge and response protocols allow manufacturers to ensure that vehicles are in a secure condition before any repairs are made. *Id.* at 22. And because manufacturers are involved in the authorization process for software and firmware updates made through the port, manufacturers also can ensure that any scan-tool update is done with a manufacturer-approved fix to resolve the vehicle's issue safely. *Id.* at ¶ 21.

Authentication controls. These controls (such as secure keys or encryption keys) are an additional manufacturer design element that keep safety-critical and emissions-control systems secure. When an ECU transmits a message, it also sends a secure key. FoF ¶ 26. The receiving ECU will then verify the secure key to ensure that the message was not manipulated in any way while in transit. *Id.* If the key is missing, the ECU will enter fail-safe mode—presenting a range of options from ignoring the message to reducing engine power or blocking further messages for a certain period of time. *Id.* In this way, secure keys help to prevent threat actors from transmitting malware or other unauthorized communications that may affect a vehicle's safety- or emissions-critical functions. *Id.* at ¶ 27.

2. The Data Law upends the robust system of manufacturer cybersecurity controls—immediately, and at pain of substantial penalty. FoF ¶¶ 15, 82, 104; CoL ¶¶ 22, 33.

Massachusetts' prior Right to Repair law mandated that motor vehicle manufacturers "provide access to their onboard diagnostic and repair information system" via software that could be used on "an off-the-shelf personal computer" and one of several hardware options, including "a non-proprietary vehicle interface device" that complies with SAE J2534. Mass. Gen. L. ch. 93K, § 2(d)(1); *see* CoL ¶ 10. Anyone with that access can both read and write to vehicles' on-board diagnostic ("OBD") systems to the extent necessary to diagnose, maintain, and repair motor

vehicles. CoL ¶¶ 83-84; Affidavit of Steven Douglas ("Douglas Aff.") at ¶ 10.

Section 2 of the Data Law expands requirements for that access. Among other things, it mandates that such "access" be "standardized." FoF ¶ 87; CoL ¶¶ 16-20. According to the Attorney General, "standardized" means there must be "a common, agreed upon way of communicating." Attorney General's Substitute Proposed Findings of Fact and Conclusions of Law ("AG FoF" / "AG CoL") at ¶ 62. Section 2's requirement of standardized access mandates that the hardware and software needed to read and write to vehicles' OBD systems must be made uniform across all vehicles sold in the Commonwealth by any manufacturer. FoF ¶ 87; CoL ¶¶ 16-20.

Section 2 also states that the access must "not require any authorization by the manufacturer, directly or indirectly"—such that, according to the Attorney General, the vehicle manufacturer cannot impose *any* restrictions on what users "[are] and [are] not permitted to do on [the OBD] system" (AG FoF ¶ 54)[4]—unless two conditions are met:

- First, "the authorization system for access to vehicle networks and their on-board diagnostic systems" must be "standardized across all makes and models sold in the Commonwealth." Data Law § 2. Thus, *all* vehicles sold by *any* manufacturer in Massachusetts must have standardized access not only to on-board diagnostics systems, but also vehicle networks, including all of their CAN bus networks, local interconnect networks, and external-facing networks. FoF ¶ 87; CoL ¶¶ 16-20;

- Second, that standardized authorization system must also be "administered by an entity unaffiliated with a manufacturer"—*i.e.*, an entity that is outside of the direct or indirect control of the manufacturer. AG FoF ¶ 56.

Likewise, Section 3 of the Data Law requires that motor vehicles with telematics systems from model year 2022 onward must meet certain new requirements. FoF ¶¶ 97-98; CoL ¶ 24. Thus, those vehicles' newly required "platform"—which (according to the Attorney General) includes

[4] The Attorney General contends that "authorization" does not also include "authentication," which the Attorney General defines as "the confirmation of the identity of an individual, user, or other actor." AG FoF ¶ 54. But the Data Law does not contain any reference to "authentication," and the Attorney General's argument ignores that appropriate authorization cannot be granted without authenticating users. *E.g.*, Affidavit of Bryson Bort ("Bort Aff."), at ¶ 53.

their "vehicle architecture and associated software/features" (AG FoF ¶ 60)—must be:

- "inter-operable," which the Attorney General defines as a "standard way to connect and communicate with the vehicle" and the platform that "can be used regardless of the manufacturer" (*id.* at ¶ 61);
- "standardized," which the Attorney General defines as "a common, agreed upon way of communicating" (*id.* at ¶ 62); and
- "open access," which the Attorney General defines as "a non-gated way to gain access to the [vehicle's] data and capabilities" (*id.* at ¶ 63).

That platform also must be "[d]irectly accessible by the owner through a mobile-based application," *i.e.*, an application on a mobile device. And it must be "[c]apable of securely communicating all mechanical data emanating directly from the motor vehicle via a direct connection to the platform," FoF ¶ 97; CoL ¶ 28—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," Data Law § 1; *see also* FoF ¶ 97; CoL ¶¶ 12, 14, 28. Moreover, if the vehicle owner authorizes it, that "mechanical data" must be "directly accessible" to an independent repair facility for the time needed to maintain, diagnose, and repair the vehicle. FoF ¶ 97; CoL ¶ 26. Again, that "access" must be provided on both a read/write basis—so users will have "the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair." FoF ¶ 97; CoL ¶ 27.

The requirements in Sections 2 and 3 of the Data Law are fundamentally inconsistent with the cybersecurity controls that manufacturers already employ to protect safety- and emissions-critical functions to comply with federal motor vehicle safety standards ("FMVSSs"). FoF ¶¶ 17-81, 88-89, 92-133; CoL ¶¶ 57, 68.

First, the Attorney General and her experts admit that the systems required immediately by the Data Law simply do not exist. FoF ¶¶ 91, 104; CoL ¶¶ 23, 30. There is no currently existing

system architecture that allows standardized access to all aspects of vehicle OBD systems, much less one that does not require any authorization by the manufacturer, directly or indirectly. FoF ¶ 91; Affidavit of Mark Chernoby ("Chernoby Aff.") at ¶ 64; Affidavit of Kevin Tierney ("Tierney Aff.") at ¶ 85. Nor is there any currently existing system architecture that would allow access to all "vehicle networks" (Data Law § 2) that is administered by a third-party unaffiliated with a manufacturer. *Id.* Nor is there any currently existing "platform" that would allow for the "inter-operable, standardized and open access" to all vehicle data otherwise related to vehicle diagnosis, repair, or maintenance. FoF ¶ 104; Chernoby Aff. ¶ 79; Tierney Aff. ¶ 88.

Second, the Data Law's standardization is directly contrary to manufacturers' existing controls because it precludes diversity in cybersecurity approaches, which is critical for manufacturers to stay ahead of hackers. FoF ¶¶ 129-30. For SAE J2534 access to OBD systems, manufacturers have adopted different messaging protocols for communications among vehicle components. *E.g.*, Bort Aff. ¶ 64. To take control of vehicle functions, then, a threat actor must reverse engineer the messaging protocols for each manufacturer, including across different makes and model years. *Id.* at ¶ 65. But standardization in the Data Law requires manufacturers to abandon their differing protocols or develop a solution that translates these messages to a standard language—so that once threat actors could decode the messages on one vehicle system, they could do the same on all vehicles across the entire industry, significantly magnifying risk. *Id.*

Third, the only way that manufacturers could comply with Sections 2 and 3 would be to abandon or degrade cybersecurity controls around safety- and emissions-critical functions, including challenge and response protocols, authentication controls (like secured keys), and secured gateways and internal firewalls within those gateways. FoF ¶¶ 113-14, 117-28. After all, current cybersecurity protections rely on manufacturer involvement in the chain of authorization

(and thus the chain of authentication), which the Data Law prohibits. *Id.* at ¶¶ 106, 115-16. And those protections are antithetical to the "open access" regime to all data otherwise related to the diagnosis, repair, or maintenance of the vehicle that the Data Law requires. *Id.* at ¶¶ 111-12.

To take just one example, under the Data Law, manufacturers would not be permitted to maintain a secured gateway that segregates communications between telematics ECUs and vulnerable, safety-critical ECUs because the Data Law mandates ready third-party access to both. FoF ¶¶ 117-19; *see also* Bort Aff. ¶ 101. Layered on top of that, the Data Law's standardization requirements expand the risks posed by threat actors, and the law's requirements of access to "vehicle networks" (as well as OBD systems) would permit those actors to modify nearly all elements of the vehicle, including additional elements of safety- and emission-critical systems not accessible under the existing law. *E.g.*, Bort Aff. ¶¶ 62-65. Threat actors would have free rein to compromise vehicle safety and emissions performance. *Id.* at ¶¶ 65. 75; Tierney ¶ 97.

The Attorney General and her experts reach a contrary conclusion only by ignoring the plain language of the Data Law when it suits them, proposing "solutions" that do not comply with the Data Law's requirements, are untested, or both, and concocting a series of hypothetical interim measures that depend on third parties to implement unproven methods that are not currently used in *any* vehicle. *See* AG FoF ¶¶ 18-27, 37, 53, 189-94, 200-05, 229-42.[5]

For instance, the Attorney General ignores that if the manufacturer requires authorization

[5] The Attorney General also proposes to slice the Data Law into discrete parts to try to preserve as much of it as possible. AG CoL ¶¶ 106-07. As authority, she points to cases involving review of federal statutes. *Id.* But when a state law is at issue, "[s]everability is of course a matter of state law." *Leavitt v. Jane L.*, 518 U.S. 137, 139 (1996). Under Massachusetts law, the Data Law rises or falls as a whole. *See* CoL ¶¶ 80-81. The Data Law contained no severability clause, and even if it had, Massachusetts has never enforced such a clause in a ballot initiative. *See Abdow v. Attorney General*, 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 imitative." *Anderson v. Attorney General*, 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).

to the vehicle's OBD system, the manufacturer must surrender that right to a third party (which doesn't exist), who then must be able to grant access not just to the OBD system, but to all "vehicle networks." AG FoF ¶ 53. Similarly, for purposes of Section 3, the Attorney General writes out of the Data Law's definition of "[m]echanical data" the qualifier that it encompasses data "*otherwise related to* the diagnosis, repair, or maintenance of the vehicle," which necessarily makes the data (and thus system access) broader than simply "diagnosis, repair, or maintenance data." *Id.* at ¶ 37.

She also posits that manufacturers could comply with Section 3 by disabling telematics systems. AG FoF ¶¶ 200-05. But that would merely avoid compliance with those requirements through the cessation of normal business operations—an obligation that preemption principles do not impose on plaintiffs bringing a preemption challenge. *See* CoL ¶ 31. Moreover, disabling telematics systems would introduce a whole host of its own safety concerns, FoF ¶¶ 12, 101-02—including allowing manufacturers to ensure that vehicle software is up to date and depriving Massachusetts vehicle owners of valuable services, such as emergency crash notification, *id.* at ¶ 101. And that is to say nothing of the practicalities of somehow doing so for all vehicles sold in Massachusetts—and yet only for vehicles in Massachusetts—without transforming the Data Law into an (unconstitutional) extraterritorial mandate. *See* CoL ¶ 29.

And the Attorney General's various "solutions" for a viable third-party cybersecurity regime depend on (1) unproven, theoretical systems that are not nearly ready for deployment in the real world—Secure Vehicle Interface ("SVI"), which has never been tested or implemented in the field, AG FoF ¶¶ 229-42; FoF ¶ 105; (2) voluntary projects limited to undertakings such as vetting locksmiths, which even on that limited scale have had security problems—the Secure Data Release Model ("SDRM") run by the National Automotive Service Task Force ("NASTF"), *id.* at ¶¶ 189-94; FoF ¶¶ 107-09; and (3) a hypothetical public key infrastructure ("PKI") system for

managing secure keys that would remove the one entity (manufacturers) best able and incentivized to protect their vehicles from cyberattack, with predictably dire consequences for vehicle safety and emissions protection, AG FoF ¶¶ 18-21; FoF ¶ 106.

B. The Data Law Conflicts with the Purposes and Objectives of the Safety Act.

The Data Law's requirement that manufacturers remove or otherwise degrade key cybersecurity controls that protect safety-critical vehicle functions "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Oneok, Inc. v. Learjet, Inc.*, 575 U.S. 373, 377 (2015); *see also* CoL ¶ 39. Obstacle preemption is "context" specific, involving a "search for the objectives that underlie" the particular federal law at issue. *Grant's Dairy—Maine, LLC v. Comm'r of Main Dep't of Agr., Food, & Rural Res.*, 232 F.3d 8, 15-16 (1st Cir. 2000).[6] As one court put it, the analysis "requires the court independently to consider national interests and their putative conflict with state interests." *Columbia Venture, LLC v. Dewberry & Davis, LLC*, 604 F.3d 824, 829-30 (4th Cir. 2010). *See* CoL ¶¶ 39-42.[7]

The Data Law would require manufacturers to take steps counter to the purposes and objectives of the Safety Act. FoF ¶¶ 64-79. NHTSA has made clear that a failure to maintain adequate cybersecurity controls would give rise to a safety-related defect, and therefore recall

[6] As commentators have observed, a law "might be impliedly preempted because it creates an impermissible obstacle to achievement of federal statutory objectives and purposes, even if [it] is not at odds with the text of governing federal laws." Gillian E. Metzger, *Federalism and Federal Agency Reform*, 111 Colum. L. Rev. 1, 15 (2011); *accord* Kenneth W. Starr, *Reflections on* Hines v. Davidowitz*: The Future of Obstacle Preemption*, 33 Pepp. L. Rev. 1, 6 (2006).

[7] In this way, the Supremacy Clause operates as a check on state incursion into national matters. Although states enjoy some leeway to take "complementary action," matters impacting interstate commerce are lodged decidedly in the federal domain. Thomas Reed Powell, Vagaries & Varieties in Constitutional Interpretations 176 (2002); *see also id.* at 164 ("Such powers as the states enjoy over [interstate] commerce derive *aliunde*, and the fact that interstate commerce is thereby regulated is a hurdle or a barrier rather than a justification. The judgment as to the height of the barrier and as to the desirability of being permitted to surmount it is not a judgment that the state is free to make as it chooses."). *See* CoL ¶ 36. The concept is not unlike the dormant commerce clause, which similarly recognizes the "compelling need for national uniformity in regulation." *Gen. Motors Corp. v. Tracy*, 519 U.S. 278, 299 n.12 (1997). In that context, a state law may not "impose[] a burden on interstate commerce that outweighs any benefits received." *Grand River Enters. Six Nations, Ltd. v. Beebe*, 574 F.3d 929, 942 (8th Cir. 2009) (citing *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970)). Here, rather than the burden on interstate commerce, the relevant consideration is the burden imposed on the achievement of the federal law's purposes and objectives.

obligations under the Safety Act. *Id.* ¶¶ 64-72, 110-29. And the Data Law's requirements cannot be satisfied by manufacturers without removing current cybersecurity controls that are critical for maintaining vehicle safety. *Id.* ¶¶ 17-44, 53, 56, 59, 62, 89, 113-14, 110-28.

Congress passed the Safety Act over a half century ago to "reduce traffic accidents and deaths and injuries resulting from traffic accidents." 49 U.S.C. § 30101. The Act delegated authority to the Secretary of Transportation, who in turn delegated it to NHTSA. 49 C.F.R. § 1.95(a). With the "broad authority granted to" it by Congress, *Verna by Verna v. U.S. Suzuki Motor Corp.*, 713 F. Supp. 823, 827 (E.D. Pa. 1989), NHTSA focuses on its core objectives—"saving lives, preventing injuries, and reducing economic costs resulting from road traffic crashes through education, research, safety standards, and other enforcement activity," *Butler v. Daimler Trucks of N.A., LLC,* 433 F. Supp. 3d 1216, 1241 (D. Kan. 2020).

The Safety Act confers twin authorities on NHTSA for the purpose of protecting the safety of motor vehicles: (1) to issue and enforce FMVSSs for new vehicles and equipment, 49 U.S.C. § 30111, which expressly preempt inconsistent state or local laws, *id.* at § 30103(b); (2) to require manufacturers to issue notification and remedy campaigns—commonly called recalls—to address and remediate safety-related defects arising in vehicles, *id.* §§ 30118-120. The Act requires manufacturers to initiate recalls when either NHTSA *or the manufacturer* identify a defect, *id.* §§ 30118(a), 30120(a), ultimately authorizing NHTSA to order a recall if the manufacturer does not commence one, *id.* § 30118(b)(2). NHTSA achieves its agency objectives through its exercise of these twin authorities.[8] CoL ¶¶ 46-47.

[8] As NHTSA recently noted, the "Safety Act defines 'motor vehicle safety' as 'the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle.'" 85 Fed. Reg. 83143, 83150 (Dec. 21, 2020) (quoting 49 U.S.C. 30102(a)(9)). That "common term"—vehicle safety—"is the driving force behind both FMVSS-setting and defect determinations, act[ing] to link NHTSA's execution of its authorities against unreasonable safety risks inherently, both in setting FMVSS and in overseeing the safety of vehicle design, construction, and performance." *Id.*

Recalls help NHTSA ensure that any safety-related defects are remedied. 49 U.S.C. §§ 30118-120. Manufacturers also have a statutory obligation to monitor safety and notify NHTSA of any safety-related defects. *E.g.*, *id.* § 30118(c). If NHTSA determines that a recall is required under the Safety Act, a state is preempted from requiring the manufacturer to create or maintain the vehicle condition giving rise to the recall because, under such circumstances, it would be impossible to comply with both the Safety Act and the state law. CoL ¶ 48.

NHTSA also enforces its regulatory objectives proactively, *before* a recall for a safety-related defect is needed. FoF ¶¶ 65, 71; CoL ¶¶ 50-51. To do so, NHTSA occasionally publishes guidance for the automotive industry that it regulates on the agency's interpretation of the term "defect related to motor vehicle safety," 49 U.S.C. § 30118(b)(1), as that term applies in particular contexts or to particular conditions. CoL ¶ 50.

A few years ago, for example, NHTSA issued guidance confirming that, if an aftermarket software update were to create or introduce an unreasonable safety risk to motor vehicle systems, "then that safety risk constitutes a defect compelling a recall." NHTSA, *Enforcement Guidance Bulletin*, 81 Fed. Reg. 65705, 65709 (Sept. 23, 2016). Immediately after that, NHTSA released detailed cybersecurity guidance, in which the agency encouraged "proactively adopting and using available guidance such as this document and existing standards and best practices" to ensure adequate cybersecurity protection Exhibit 3 (NHTSA *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016)), at 5. Although styled as guidance, NHTSA was unequivocal that "motor vehicle and motor vehicle equipment manufacturers are required by the National Traffic and Motor Vehicle Safety Act, as amended, to ensure that systems are designed free of unreasonable risks to motor vehicle safety, including those that may result due to existence of potential cybersecurity vulnerabilities." *Id.* Thus, NHTSA has recognized the statutory requirement to maintain adequate

vehicle cybersecurity, but declined to codify particular cybersecurity controls in a regulation to allow the industry to react nimbly to the evolution of cybersecurity threats. CoL ¶ 52.

Although agency guidance does not itself have preemptive effect, the Supreme Court has recognized that an agency's views are highly probative in determining preemption because the agency "is likely to have a thorough understanding of its own regulation and its objectives and is uniquely qualified to comprehend the likely impact of state requirements." *Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 883 (2000).[9] And agency guidance provides insight into what an agency views the purposes and objectives of the statute to be. CoL ¶ 53.

NHTSA has cleared away any doubt that it views maintaining adequate cybersecurity controls as mandatory, because the agency has enforced its view that manufacturers must install and maintain appropriate cybersecurity controls to avoid the exercise of NHTSA's recall authority under 49 U.S.C. §§ 30118-120. In 2015, NHTSA found that some Chrysler vehicles had a flaw in their radio software security that could allow unauthorized third-party access to some networked vehicle control systems, exposing the driver, the vehicle occupants or any other individual or vehicle with proximity to the affected vehicle to a potential risk of injury. CoL ¶ 54. Ultimately, Chrysler worked with NHTSA to issue a voluntary recall of 1,410,000 vehicles to repair the software vulnerability and avoid a finding of a statutory violation. *See* FoF ¶¶ 67-71. Among other things, in response to that recall, Chrysler sped up the deployment of a secured gateway across its vehicle lineup, *id.* at ¶ 70—one of the cybersecurity protections that it would have to remove to comply with the Data Law's broad data access regime, *id.* at ¶ 117.

And, finally, NHTSA has specifically observed that the Data Law implicates motor vehicle safety concerns. Although manufacturers retain some flexibility in precisely how to safeguard

[9] The same goes for statutes that agencies administer. *E.g.*, *Catskills Mountains Chapter of Trout Unlimited, Inc. v. E.P.A.*, 846 F.3d 492, 520-21 (2d Cir. 2017); *accord Goncalves v. Reno*, 144 F.3d 110, 126 n.20 (1st Cir. 1998).

safety-critical vehicle systems, the agency has said that those systems must be protected in ways that are antithetical to the requirements of the Data Law—*e.g.*, through manufacturers controlling access to firmware that executes core vehicle functions such as acceleration, braking, and steering; isolating vehicle systems from one another; and maintaining non-standardized approaches across the industry to prevent large-scale hacking. *See* FoF ¶¶ 64-79, 110-29.

C. The Data Law Conflicts with the Safety Act's "Make Inoperative" Provision.

The Data Law is also preempted on conflict-preemption grounds for a separate reason. It conflicts directly with a Safety Act provision that prohibits manufacturers from making inoperative design elements like cybersecurity controls that protect safety-critical functions regulated by FMVSSs. 49 U.S.C. § 30122(b); *see, e.g.*, *Geier*, 529 U.S. at 866 (holding state law liability preempted because it "conflicts with the objectives of [an] FMVSS").

NHTSA's FMVSSs regulate several safety-critical vehicle functions. FoF ¶ 52. These standards reach broadly to include every component. For example, the FMVSS for accelerator control systems encompasses "all vehicle components, except the fuel metering device, that regulate engine speed in direct response to movement of the driver-operated control and that return the throttle to the idle position upon release of the actuating force." 49 C.F.R. § 571.124; CoL ¶ 64.

The Safety Act prohibits manufacturers from removing or degrading cybersecurity controls that protect functions regulated by FMVSSs. 49 U.S.C. § 30122(b). A "manufacturer . . . may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard prescribed under this chapter." *Id.* By its plain terms, this applies not only to features specifically identified in an FMVSS, but to "*any* . . . element of design" that the manufacturer "installed on or in a motor vehicle" to comply with the FMVSS. *Id.* (emphasis added); *see* CoF ¶¶ 60-61.

Manufacturers have installed a variety of cybersecurity protections as elements of design

of FMVSS-regulated vehicle functions—including the including challenge and response protocols, authentication controls such as secured keys, and secured gateways discussed above. FoF ¶¶ 14-45, 52-53, 55-56, 58-59, 61-62. Specifically, manufacturers' cybersecurity design elements protect core vehicle functions like acceleration, braking, steering, and airbag deployment. 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). Given the current electronic nature of safety-critical functions, these cybersecurity controls help to prevent threat actors (or others) from taking control of the functions and, ultimately, the vehicle itself—without which manufacturers could not comply with several FMVSSs (*see* CoL ¶¶ 64-67):

- The safety standard for **acceleration control systems (FMVSS 124)** presupposes that *the driver*—not some threat actor—will be in control of a vehicle's acceleration, describing the function that it covers as a "*[d]river*-operated accelerator control system" and "establishes the requirement for the return of a vehicle's throttle to the idle position when *the driver* removes the actuating force from the accelerator control." 49 C.F.R. § 571.124 (emphasis added).

- The safety standard for **electronic stability control ("ESC") systems (FMVSS 126)**, which governs steering and anti-lock braking via a "computer using a closed-loop algorithm to limit vehicle oversteer and to limit vehicle understeer," presupposes that electronic inputs come from *the driver*, and that *the driver* remain in control, describing the approved system as a "means to monitor *driver* steering inputs" that requires the "algorithm to determine the need, and a means to modify engine torque, as necessary, to assist *the driver* in maintaining control of the vehicle," as well as retain *the driver*'s ability "disable[] the ESC" system). *Id.* § 571.126 (emphasis added).

- The safety standard for **light-vehicle brake systems (FMVSS 135)**, which has the broad purpose of "insuring safe braking performance under normal and emergency conditions," presupposes that *the driver*—not some threat actor—remains in control of a vehicle's braking, describing the function that it covers as involving the "*driver* action . . . of modulating the energy application level" to the brake, discussing brake testing conditions to include "[p]edal force . . . applied and controlled by *the vehicle driver*," and any assistance feature must ensure that while "reduc[ing] the amount of muscular force that *a driver* must apply to actuate the system" it "does not prevent *the driver* from braking the vehicle by a continued application of muscular force." *Id.* § 571.135 (emphasis added).

- The safety standard **occupant crash protection (including air bags) (FMVSS 208)** contemplates that the air bags will deploy when the "vehicle is in a crash severe enough to cause the air bag to inflate"—not when a threat actor activates them. *Id.* § 571.208.

Because of the Data Law, manufacturers would have to remove or otherwise degrade cybersecurity control design elements that they installed to ensure that these safety-critical functions operate as intended. FoF ¶ 14-45, 52-53, 55-56, 58-59, 61-62; CoL ¶¶ 58-68.

D. The Data Law Conflicts with the Clean Air Act.

For similar reasons, the Data Law conflicts with the requirements, purposes, and objectives of the Clean Air Act. Congress's principal purpose was to "protect and enhance the quality of the Nation's air resources so as to promote the public health and welfare and the productive capacity of its population." 42 U.S.C. § 7401(b)(1). The Data Law's required changes to vehicle cybersecurity protection would more readily allow vehicle owners or others access to a vehicle's engine control module to disable emissions control systems via aftermarket software. FoF ¶¶ 76-80. Those changes run directly counter to Congress's purposes and objectives. CoL ¶¶ 69-78.

The Data Law would also require manufacturers to render inoperative cybersecurity design elements installed on vehicles to meet the requirements of the Clean Air Act and Environmental Protection Agency ("EPA") regulations regarding vehicle emissions. FoF ¶ 78; CoL ¶¶ 73, 79.

In Clean Air Act, Congress established a comprehensive statutory regime to control air pollution from all national sources. 42 U.S.C. §§ 7401, *et seq.* The Act carefully delineates responsibilities between the federal government and the states. With limited exceptions inapplicable here, Title II of the Act, 42 U.S.C. §§ 7521-90, vests the federal government with exclusive authority to regulate mobile sources such as vehicles. The Act imposes stringent vehicle emissions requirements on manufacturers including warranting the emission control system for the vehicle's "useful life"—either 10 years or 100,000 miles. *Id.* §§ 7521(d), 7541(a)(1). Manufacturers must test post-sale vehicles at regular mileage intervals. 42 C.F.R. § 86.1845-04. And EPA can make manufacturers change vehicle configurations, including software, to ensure that vehicles continue to meet federal emissions-control limits. *See id.* § 86.1842-01(b); CoF ¶ 72.

Under the Clean Air Act, it is a violation of federal law for "any person to remove or render inoperative any device or element of design installed on or in a motor vehicle engine in compliance with regulations under [the Act] prior to its sale and delivery to the ultimate purchaser, or for any person knowingly to remove or render inoperative any such device or element of design after such sale and delivery to the ultimate purchaser." 42 U.S.C. § 7522(a)(3)(A). As in the Safety Act, the language of the Clean Air Act broadly encompasses "*any* . . . element of design." *Id.* (emphasis added). The element of design need not itself be explicitly required by regulations, but merely one "installed . . . in compliance with regulations." *Id.*; *see also* 40 C.F.R. § 86.1803-01 ("element of design" includes "any control system (*i.e.*, computer, software, electronic control system, emission control system, computer logic)" in the vehicle). CoL ¶¶ 73-75.

Manufacturers have installed cybersecurity protections around the engine control module that are key "element[s] of design" of vehicles, which allow them to comply with Clean Air Act standards. 42 U.S.C. § 7522(a)(3)(A). FoF ¶ 78. The Data Law's requirements (and timeline to meet those requirements) will, if permitted to take effect, require manufacturers to eliminate or significantly degrade existing cybersecurity controls installed in vehicles to protect against cyber intrusion of emissions-related vehicle components. FoF ¶¶ 72-78; CoL ¶¶ 72-80. That would conflict with the requirements, purposes, and objectives of the Clean Air Act. CoL ¶¶ 69-79.

E. Plaintiff Is Entitled to Equitable Relief on Its Preemption Claims.

Auto Innovators properly seeks declaratory and injunctive relief for the constitutional violations it asserts. CoL ¶¶ 83-87.[10] An injunction should issue. *See id.* at ¶ 84.

[10] The Attorney General includes a new, scattershot argument that this Court lacks the equitable power to entertain this preemption claim. Relying on *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320 (2015), and its progeny, the Attorney General says that Auto Innovators must be able to point to a substantive federal right conferred on auto manufacturers in the Safety Act or Clean Air Act. *See* AG CoL ¶¶ 16-17. First, the *Armstrong* line of cases is inapplicable. *Armstrong* involved a plaintiff that was seeking an affirmative benefit to a more favorable Medicaid reimbursement rate determination allegedly available under federal law—far afield from a claim that it was subject to conflict obligations that impose quasi-criminal penalties. *See Armstrong*, 575 U.S. at 324-25; *accord Safe Streets*

First, the Data Law would inflict irreparable injury. As discussed, manufacturers have federal-law duties they would have to violate comply with the Data Law—subjecting them to penalties under federal law. And if they continued to follow federal law, they would violate the Data Law. Compliance with one requires violation of the other. *Second*, the balance of hardships weighs in favor of equitable relief. The cybersecurity threats resulting from the Data Law would daily put at risk manufacturers' reputations in a competitive industry, with incalculable costs. Chernoby Aff. ¶ 77; Tierney Aff. ¶¶ 108-10. Plus, manufacturers already provide access to any vehicle data necessary for diagnosis, repair, or maintenance. FoF ¶ 83. *Finally*, protecting public health and safety is in the public interest, as is halting the enforcement of unconstitutional laws. *See, e.g.*, *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013). *See generally* CoL ¶¶ 83-87.

II. Auto Innovators Has Associational Standing to Seek Relief.

The Attorney General does not dispute that individual manufacturers meet Article III standing requirements to challenge the Data Law in their own right. *See* AG CoL ¶¶ 3-9.[11] That leaves only the third associational standing prong, which is merely prudential. CoL ¶ 5.

Alliance v. Hickenlooper, 859 F.3d 865, 902 (10th Cir. 2017) (cited at AG CoL ¶ 15) (plaintiffs could not maintain equitable preemption claim asserting that Colorado's marijuana law is preempted by federal law because they did not have a substantive right to a benefit under the federal law).

By contrast, where, as here, the claim is that it is impossible *to comply* with the two laws, *Armstrong*'s logic does not apply. *See, e.g.*, *Friends of the East Hampton Airport, Inc. v. Town of East Hampton*, 841 F.3d 133, 146 (2nd Cir. 2016) (*Armstrong* did not mandate dismissal of preemption claims though challenged statute conferred enforcement authority on the FAA, because plaintiffs did not seek "to enforce the federal law themselves, but to preclude a municipal entity from subjecting them to local laws enacted in violation of federal requirements"). Unsurprisingly, then, outside the narrow context of *Armstrong* and cases like it, courts allow private preemption challenges. *See, e.g.*, *Capron v. Office of Atty. Gen. of Mass.*, 944 F.3d 9 (1st Cir. 2019); *Algonquin Gas Transmission, LLC v. Weymouth*, 919 F.3d 54 (1st Cir. 2019); *Consumer Data Indus. Ass'n v. Frey*, 495 F. Supp. 3d 10 (D. Me. 2020).

In any event, neither the Safety Act nor the Clean Air Act contain provisions that evince an intent to foreclose this type of equitable relief, nor are they "judicially unadministrable" (575 U.S. at 328) like the Medicaid statute in *Armstrong*. *See, e.g.*, *Hurley v. Motor Coach Indus., Inc.*, 222 F.3d 377, 382-83 (7th Cir. 2000); *Griffith v. Gen. Motors Corp.*, 303 F.3d 1276 (11th Cir. 2002); *Minn. Auto. Dealers Ass'n v. Stine,* 2016 WL 5660420, at *8 (D. Minn. Sept. 29, 2016) (specifically addressing *Armstrong*).

[11] Nor could she. Sections 2 and 3 of the Data Law impose extensive obligations on manufacturers. And the interests Auto Innovators seeks to vindicate in this suit are pertinent to the objectives for which it was formed. FoF ¶¶ 1-4.

The Attorney General complains about the scope of discovery. AG CoL ¶¶ 5-6, 8-9. But it is unrealistic to think that every manufacturer would participate in the discovery process for this case. *Contra* AG CoL ¶ 9. That would have been a logistical nightmare, substantially delayed this expedited trial, and ultimately defeated the entire point of associational standing. Consistent with this Court's direction to have a limited number of fact witnesses, Auto Innovators necessarily limited the number of participating manufacturer members to a couple representative samples from the more than a dozen that filed affidavits in support of a preliminary injunction.

The Attorney General has had nearly unfettered access to all of the information it wanted from two of the largest automakers in the country. Both of those automakers employ a rigorous approach of layered cybersecurity controls, including the ones discussed above. *Contra* AG CoL ¶ 7. And Auto Innovators' members are aligned in their inability to comply with both the Data Law and federal law as well as in their cybersecurity concerns about harm that would come from an attempt to implement the Data Law. *See, e.g.*, FoF ¶¶ 2-4, 5-16, 19-29, 33-37, 44-45, 52-63, 65-66, 73-80, 81-84, 91-95, 100, 102, 104-09, 111-14, 118-24, 126, 130. That alignment was made crystal clear at the preliminary injunction stage—showing the broad agreement across the auto industry that manufacturers could not comply simultaneously with federal law and the Data Law.[12]

CONCLUSION

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

[12] Moreover, the relief that Auto Innovators seeks on behalf of its members confirms associational standing. CoL ¶¶ 6-7. Auto Innovators speaks on behalf of the auto industry as a whole, not one particular manufacturer, and the declaratory and injunctive relief it seeks would benefit the auto industry as a whole. *Id.* at ¶ 4; Douglas Aff. ¶¶ 2-3.

Dated: June 4, 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 4, 2021.

/s/ Laurence A. Schoen