IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, *Plaintiff*, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, *Defendant.*	No. 1:20-cv-12090-DPW

BRIEF OF IFIXIT, THE REPAIR ASSOCIATION, U.S. PIRG EDUCATION FUND, INC., SECUREPAIRS.ORG, THE ELECTRONIC FRONTIER FOUNDATION, AND PROFESSOR JONATHAN ASKIN AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT

Christopher T. Bavitz (BBO #672200)
Cyberlaw Clinic, Harvard Law School
1585 Massachusetts Ave.
Cambridge, MA 02138
Tel: (617) 384-9125
Email: cbavitz@law.harvard.edu

Counsel for Amici Curiae

June 7, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

Other Sources

John Lypen, *Editor's Report—Automotive Statistics—Independent Aftermarket*, Motor (May 2019), https://www.motor.com/magazine-summary/editors-report-may-2019/ 16

Marianne Kolbasuk McGee, *EHR Interoperability Plan Raises Concerns*, GovInfo Security (Apr. 7, 2015), https://www.bankinfosecurity.com/ehr-interoperability-plan-raises-concerns-a-8082 6

Charlie Miller & Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* (Aug. 10, 2015), http://illmatics.com/Remote%20Car%20Hacking.pdf 10

Phil Muncaster, *Over Three Million US Drivers Exposed in Data Breach*, Infosecurity Mag. (Feb. 3, 2021), https://www.infosecurity-magazine.com/news/over-three-million-us-drivers/ 12

Office of the Nat'l Coordinator for Health Info. Tech., *Report on Health Information Blocking* (Apr. 2015), https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf 6

Aaron Perzanowski, *Consumer Perceptions of the Right to Repair*, 96 Ind. L.J. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584377 . . . . . 13, 16

Aaron Perzanowski & Jason Schultz, *The End of Ownership: Personal Property in the Digital Economy* (2016) 14

Jay Peters, *Volunteers Produce 3D-Printed Valves for Life-Saving Coronavirus Treatments*, The Verge (Mar. 17, 2020), https://www.theverge.com/2020/3/17/21184308/coronavirus-italy-medical-3d-print-valves-treatments 16

Press Release, AutoMD, *Dealership or Repair Shop? AutoMD.com Debunks Top Five Myths* (May 17, 2010), https://www.automd.com/about-automd/articles/dealership-or-repair-shop/ 15

Nathan Proctor, *Half of U.S. States Looking to Give Americans the Right to Repair*, U.S. PIRG (Mar. 10, 2021), https://uspirg.org/blogs/blog/usp/half-us-states-looking-give-americans-right-repair 17

Nathan Proctor, U.S. PIRG Educ. Fund, *The Fix Is In: How Our Smartphones Get Fixed, Why It's Harder Than It Should Be, and Why That Matters* (Mar. 2020), https://uspirg.org/sites/pirg/files/reports/The-Fix-Is-In/The_Fix_Is_In_March2020_USPEF.pdf 17

Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents*, 2 J. Cybersecurity 121 (2016) 11

Karen Scarfone et al., *Spec. Pub. 800-123*, *Guide to General Server Security* (Nat'l Inst. of Standards & Tech. July 2008), https://csrc.nist.gov/publications/detail/sp/800-123/final . 11

Stephen Shepherd, SANS Inst., *How Do We Define Responsible Disclosure?* (2003), https://www.sans.org/reading-room/whitepapers/threats/paper/932 11

Bill Siwicki, *Could HHS Information Blocking Rule Have Unintended Consequences on Data Sharing and Security?*, Healthcare IT News (Sept. 13, 2019), https://www.healthcareitnews.com/news/could-hhs-information-blocking-rule-could-have-unintended-consequences-data-sharing-and 6

Ewan Spence, *Your Broken iPhone May Wait a Long Time to Be Fixed*, Forbes (Mar. 30, 2020), https://www.forbes.com/sites/ewanspence/2020/03/30/apple-iphone-repair-delay-right-to-repair-coronavirus-covid19-social-distancing/ 15

Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 Hous. L. Rev. 1333 (2006) 10

Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927 (Fed. Commc'ns Comm'n Mar. 13, 2007), https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf 8

Tencent Keen Sec. Lab, *Experimental Security Research of Tesla Autopilot* (Mar. 2019), https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf 10

U.S. Gen. Accounting Office, *GAO/HEHS-00-123*, *Single-Use Medical Devices: Little Available Evidence of Harm from Reuse, but Oversight Warranted* (2000), http://www.gao.gov/new.items/he00123.pdf 15

U.S. Gov't Accountability Office, *GAO-19-196*, *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies* (Feb. 2019), https://www.gao.gov/assets/gao-19-196.pdf 7–8

Eric von Hippel, *Democratizing Innovation* (2005) 16

INTEREST OF *AMICI CURIAE*

iFixit[1] is an international, open-source, online repair manual for everything. iFixit's mission is to provide people with the knowledge they need to make their things work for as long as possible. iFixit represents the interests of a global community of makers, tinkerers, fixers, and repair professionals. In 2020, the iFixit community helped over 100 million people from almost every country in the world fix their devices. iFixit's strongly collaborative online community has published over 70,000 online repair guides. This massive, free resource has helped people fix everything from cellphones and game consoles to tractors and musical instruments.

The Repair Association encompasses over 72,115 subscribing members including trade associations, consumer advocacy groups, environmental advocates, and individuals, and including 397 paying members, all of whom are committed to defending the right to repair, reuse and recycle electronics products and services. The Repair Association members both buy and sell equipment and parts, and offer repair services for consumers, businesses, industry, education, and government throughout the global economy.

U.S. PIRG Education Fund, Inc. is a not for profit organization that advocates for the public interest, working to win concrete results on real problems that affect millions of lives, and standing up for the public interest against powerful interests when they push the other way. It employs grassroots organizing and direct advocacy for the public on many different issues including healthcare, preserving competition, and protecting consumer welfare.

[1]Pursuant to Local Rule 7.1(a)(2), counsel for *amici curiae* conferred with counsel for all parties to this case. Defendant consented to the filing of this brief, and Plaintiff indicated that it took no position on the filing of the brief. No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of the brief. No person or entity, other than *amici*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief. Affiliations for individual signatories are for identification purposes only.

SecuRepairs.org is an international, volunteer organization of information technology and information security professionals who support a digital right to repair. Founded in 2018, SecuRepairs counts more than 200 supporters worldwide. They include leading experts in secure software design, embedded device security, data encryption and cyber offensive and defensive practices. Since its founding, the group has served as a platform for information ("cyber") professionals to speak with one voice in support of a common Statement of Principles in the ongoing, national conversation about the rights of owners and independent repair professionals. In recent years, SecuRepairs supporters have provided expert testimony in support of the right to repair at the FTC's Nix the Fix forum as well as to state lawmakers across the country as they consider state-level right to repair measures.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked for more than 30 years to protect consumer interests, innovation, and free expression in the digital world. EFF and its more than 34,000 active donors have a strong interest in helping the courts and policymakers ensure that consumers are able to exercise traditional ownership rights in their devices, including the right to repair, and that manufacturers are not able to unfairly control the use, repair, and re-use of the products they sell.

Professor Jonathan Askin is the Founder/Director of the Brooklyn Law Incubator and Policy Clinic, and the Faculty Chair and Innovation Catalyst for the Center for Urban Busness Entrepreneurship. He has provided legal and policy counsel and strategic advice for companies that build and develop communications networks and Internet applications, as well as for other technology-oriented enterprises and startups.

INTRODUCTION AND SUMMARY OF ARGUMENT

Plaintiff's breathless invocation of various federal vehicle regulations notwithstanding, the Right to Repair Act of 2020 simply vindicates and extends longstanding consumer protection policies that are historically the province of the *states*. Massachusetts has stepped into the breach to protect its residents' interests in preserving their vehicles, limiting aftermarket monopolies, enhancing consumer choice and quality of service, growing small businesses, encouraging grassroots innovation, and protecting the environment. And it has done so in a way that complements, rather than conflicts, with federal laws, to the benefit of car owners, repair shops, and the public interest.

I. Plaintiff incorrectly asserts that the Right to Repair Act is fundamentally incompatible with its regulatory obligations related to cybersecurity and product safety. In fact, federal regulations regularly accommodate cybersecurity, data safety, and consumer access, in fields such as electronic health records, credit reports, and telephone call logs. These examples show that cybersecurity can coexist with data access, contrary to plaintiff's theory of the case that compliance with both is impossible.

II. Plaintiff's preemption claim also depends on a flawed cybersecurity theory. Plaintiff assumes that restricting access to telematics data is necessary to prevent malicious intrusions into cars and to comply with safety regulations. But cybersecurity experts regularly disfavor "security through obscurity"—systems that rely primarily on secrecy of certain information to prevent illicit access or use—because of the high, realistic risks of data breaches. And cybersecurity experts likewise support increasing consumer access to data, and enabling independent repair. It would be unwise to interpret, as plaintiff would have this Court do, the vehicle safety regulations at issue to include an obligation for vehicle manufacturers to adopt cybersecurity measures that

experts recognize as fundamentally flawed.

III. The exceptional importance of the Right to Repair Act to the protection of consumer expectations and interests, particularly against powerful dominant firms that seek to monopolize repair markets, likewise demands close scrutiny of plaintiff's claims. Consumers who invest in goods, including vehicles, legitimately expect that they can use them and repair them at will to preserve their usefulness. That expectation is backed by longstanding practice; independent repair has long been a mainstay of vehicle maintenance in the United States. Subverting that expectation by enshrining aftermarket repair monopolies would have drastic consequences for competition, consumer rights, and innovation. Insofar as product manufacturers seek to subvert that expectation by monopolizing aftermarket repair industries, states may legitimately act to protect consumers from such anticompetitive behavior.

At bottom, plaintiff's preemption argument amounts to a claim that any sufficiently complex regulatory system is a free pass to monopolize the market for repair services and deny consumers full enjoyment of the things that they own. There is no principled reason to give manufacturers this dead-hand control that could extend to numerous industries far afield from automobiles, and particularly in a manner of questionable cybersecurity. To give manufacturers this control would do a disservice to the electorate of Massachusetts that voted to protect their right to repair. This Court should not impute from the general existence of federal regulation, as a matter of law, a prohibition on legislative enhancements to the right to repair.

ARGUMENT

I. There Is No Inherent Conflict Between Repair-Facilitating Laws and Federal Safety Regulation, as Demonstrated by Other Regulatory Regimes

Plaintiff contends that access to telematics data required under the Right to Repair Act of 2020, ch. 386, 2020 Mass. Acts, irreconcilably conflicts with the NHTSA and Clean Air regulatory regimes.[2] *See* Pl.'s Trial Br. 1, June 4, 2021 (Doc. No. 173). But there is no inherent reason why a law that gives consumers access to the data of their own cars must conflict with product safety and cybersecurity regulations. Multiple other fields show that consumer data access can coexist with highly secure systems, so there is no reason why data access must be mutually exclusive to cybersecurity as plaintiff claims.

That the examples given involve federal regulations rather than a combination of federal and state laws does not diminish the relevance of the examples. Plaintiff's theory of the case is premised on a logical argument that it is "impossible . . . to comply with both" the Right to Repair Act and federal safety regulations. Doc. No. 173, at 3 (quoting *Freightliner Corp. v. Myrick*, 514 U.S. 280, 287 (1995)). But if that is so, then it should be equally impossible to comply with both data access and cybersecurity rules even if they were all federal. The examples herein prove that not to be the case.

A. Electronic Health Records

Electronic health record management systems provide perhaps the most comprehensive example of an agency balancing security and access. Personal health data is subject to strong pri-

[2]The term "telematics data" is used throughout to refer to information or capabilities that the Massachusetts law makes available to consumers and licensed repair facilities. *See* Right to Repair Act sec. 3.

vacy and security protections. *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-2(d); 45 C.F.R. § 164.306. At the same time, Congress and the Department of Health and Human Services require health record management systems to give patients access to their own data, in order to assist patients moving between hospitals and providers. *See* 42 U.S.C. § 300jj-52; 45 C.F.R. § 171.103(a)(1). In fact, recently promulgated federal rules directly address cybersecurity to ensure that system administrators can accommodate patient data access without undermining data security measures. *See* 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642, 25725–26 (Office of the Nat'l Coordinator for Health Info. Tech., Dep't of Health & Human Servs. May 1, 2020); 45 C.F.R. § 171.203.

The history of the electronic health record access rules is particularly instructive for this case. Like plaintiff's member companies, the electronic health record system vendors had a documented history of refusing to allow third-party access to records stored in their systems, with the effect of locking hospitals into one vendor, restraining competition and patient choice. *See, e.g.,* Office of the Nat'l Coordinator for Health Info. Tech., *Report on Health Information Blocking* 15–19 (Apr. 2015), https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf; Julia Adler-Milstein & Eric Pfeifer, *Information Blocking: Is It Occurring and What Policy Strategies Can Address It?*, 95 Milbank Q. 117, 119 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5339397/. Opposing efforts to give patients access to their own data, the system vendors claimed that data access would interfere with cybersecurity. *See, e.g.,* Bill Siwicki, *Could HHS Information Blocking Rule Have Unintended Consequences on Data Sharing and Security?*, Healthcare IT News (Sept. 13, 2019), https://www.healthcareitnews.com/news/could-hhs-information-blocking-rule-could-have-unintended-consequences-data-sharing-and; Mari-

anne Kolbasuk McGee, *EHR Interoperability Plan Raises Concerns*, GovInfo Security (Apr. 7, 2015), https://www.bankinfosecurity.com/ehr-interoperability-plan-raises-concerns-a-8082. Nevertheless, health regulators crafted a rule that enabled both cybersecurity and data access. Thus, enabling consumer data access does not necessarily render strong cybersecurity measures inoperative.

B. Credit Reporting

Credit rating agencies must also balance consumer data access with strong data security. The major consumer reporting agencies Experian, Equifax, and TransUnion are subject to at least three statutory schemes that all include cybersecurity components, enforced by both the Federal Trade Commission and the Consumer Financial Protection Bureau. *See* Gramm–Leach–Bliley Act, 15 U.S.C. § 6801(b); Dodd–Frank Act, 12 U.S.C. § 5531(a)–(b); 16 C.F.R. § 314.3; Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681b(a). *See generally* U.S. Gov't Accountability Office, *GAO-19-196*, *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies* 16–18, 21–22 (Feb. 2019), https://www.gao.gov/assets/gao-19-196.pdf. At the same time, they are required to give consumers annual free access to their own credit reports via a "streamlined" process, which includes the well-known website www.annualcreditreport.com. Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. No. 108-159, sec. 211(a)(1)(C)(i), 117 Stat. 1952, 1968–69 (codified at FCRA § 1681j); *see* 12 C.F.R. § 1022.136(b)(1)(i). Recognizing the need for strong cybersecurity on that website to avoid improper disclosure of credit records, CFPB has adopted regulations directed to authenticating consumers requesting their own reports. *See* 12 C.F.R. § 1022.123(a).

The response to the recent breach of Equifax data shows how requirements that consumers

have access to sensitive information do not interfere with strong cybersecurity measures. Even though regulators tightened their enforcement of cybersecurity authority over consumer reporting agencies in the wake of that breach and lawmakers called for stricter rules, there was no suggestion that consumer access to credit reports should be limited to prevent future data breaches—in fact, federal authorities encouraged consumers to take advantage of credit report access to mitigate fraud resulting from the stolen data. *See* U.S. Gov't Accountability Office, *supra*, at 30. Major risks to cybersecurity do not therefore necessitate locking consumers out of their data.

C. Telephone Call Records

Telecommunications carriers have a "duty to protect the confidentiality of proprietary information of . . . customers," and the Federal Communications Commission's implementing rules require those carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access" to that data. 47 U.S.C. § 222(a); 47 C.F.R. § 64.2010(b). Yet the Commission also recognizes that consumers often need access to their own call records in the course of billing disputes. *See* Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927, para. 19, at 6939 (Fed. Commc'ns Comm'n Mar. 13, 2007), https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf. As a result, the regulations also specify particular methods by which consumers can obtain that information by telephone, online, or in physical stores. *See* 47 C.F.R. § 64.2010(b)–(d). Carriers are thus required both to comply with cybersecurity regulations on call data and to provide consumer access to that data.

Each of these examples shows that regulatory requirements can accommodate both data security and consumer data access for even the most sensitive information. There is no inherent

reason why federal vehicle regulations must be wholly incompatible with access to telematics data under the Right to Repair Act, as plaintiff claims.

II. Interpreting Vehicle Safety Regulations to Require Secrecy in Telematics Data Would Contradict Well-Known Cybersecurity Practices

Central to plaintiff's case is the mistaken idea that secrecy in telematics information is a necessary condition of vehicle cybersecurity, and that making this information available under the Right to Repair Act to anyone beyond vehicle manufacturers and their designees (licensed dealerships or authorized third party repair shops) would create the preconditions for cars to be wrongfully accessed or operated by malign actors. As an example, plaintiff contends that complying with the Massachusetts law could allow malicious third parties to remotely accelerate or brake a car while in operation. *See* Doc. No. 173, at 15.

Initially, the causality in this argument merits close review because it is in tension with historical examples of remote attacks against vehicles, which have not depended on access to telematics data. University researchers in 2010 discovered exploitable flaws in vehicle telematics units simply by asking the cars' computers to expose the units' software; their subsequent research took advantage of software debugging features that the vehicle manufacturer had erroneously failed to remove before shipping the vehicles. *See* Karl Koscher et al., *Experimental Security Analysis of a Modern Automobile*, 2010 Proc. IEEE Symp. on Security & Privacy 447, 455 (2010), http://www.autosec.org/pubs/cars-oakland2010.pdf; Stephen Checkoway et al., *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, 20 Proc. USENIX Security Symp. 77, 86 (2011), https://static.usenix.org/event/sec11/tech/full_papers/sec11_proceedings.pdf. When Charlie Miller and Chris Valasek showed that they could remotely force a Jeep Chero-

kee to drive off the road, they analyzed that car's telematics system by presenting the system with a modified software update, which the car did not verify before installing. *See* Charlie Miller & Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* 34–38 (Aug. 10, 2015), http://illmatics.com/Remote%20Car%20Hacking.pdf; *see also* Tencent Keen Sec. Lab, *Experimental Security Research of Tesla Autopilot* 1 (Mar. 2019), https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf (discovering vulnerabilities in Tesla vehicle based on inspection of onboard software). These and other proof-of-concept attacks on vehicles relied on neither cooperation with the manufacturers[3] nor access to any of the diagnostic software, tools, schematics, or resources covered by the Right to Repair Act. Why access to telematics data under that law will affect vehicle security in view of the data's historical irrelevance will be an important question to resolve at trial.

But taking plaintiff's contentions at face value, they encounter a second problem. Information security experts widely disfavor approaches to security, such as the one put forward by the plaintiffs, that rely on secrecy as the means to prevent unwanted intrusion into technological systems—in information security industry parlance, "security through obscurity." *See, e.g.,* Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 Hous. L. Rev. 1333, 1337 (2006).[4] Rather than making sensitive software more secure by protecting it from unwanted attention, security through obscurity allows flaws and insecurity in technology to flourish by decreasing the likelihood that they will be

[3]In all of the cited examples, the researchers gave the manufacturers advance notice of the flaws after discovery but before publication, to provide time to update vulnerable cars.

[4]Swire contends that secrecy may be preferable for security where the elements to be protected are highly unique and repeat attacks are unlikely. *See* Swire, *supra*, at 1340–41. That situation is of little applicability to vehicle security, where numerous identical makes and models are simultaneously on the road.

identified and repaired, while "increas[ing] the likelihood that [flaws] can and will be exploited by evil-doers." Steven M. Bellovin & Randy Bush, *Security Through Obscurity Considered Dangerous* 1 (Internet Soc'y, Internet-Draft working paper, Feb. 28, 2002), https://www.ietf.org/archive/id/draft-ymbk-obscurity-00.txt. The National Institute of Standards and Technology recommends for computer systems that "security should not depend on the secrecy of the implementation or its components." Karen Scarfone et al., *Spec. Pub. 800-123*, *Guide to General Server Security* 2-4 (Nat'l Inst. of Standards & Tech. July 2008), https://csrc.nist.gov/publications/detail/sp/800-123/final.

Experts disfavor security through obscurity both because secrecy is unlikely to deter a capable adversary and because it allows vulnerabilities to persist undetected and uncorrected, multiplying and broadening the avenues into sensitive systems for malicious actors. *See, e.g.,* Stephen Shepherd, SANS Inst., *How Do We Define Responsible Disclosure?* 6–7 (2003), https://www.sans.org/reading-room/whitepapers/threats/paper/932. The ability of determined adversaries to discover flaws in vehicle software regardless of efforts by vehicle makers to conceal them casts serious doubt on plaintiff's contention that denying access to telematics systems for the purpose of maintenance and repair will keep vehicles secure from cyber attack or measurably improve the cybersecurity of Internet connected vehicles in any way.

Hinging nationwide vehicle security on car manufacturers' ability to keep telematics data obscured from the Right to Repair Act would be a disaster waiting to happen. There are plenty of strategies for gaining illicit access to supposedly secret data—so-called "phishing," "watering hole," and "pretexting" strategies, among others—that can fool employees into revealing usernames and passwords that give malign actors access to sensitive, internal systems. *See generally* Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents*, 2 J. Cybersecurity 121, 123

(2016). Automobile manufacturers and dealers are not unusually skilled at securing data, having suffered their fair share of data breaches. *See, e.g.,* Phil Muncaster, *Over Three Million US Drivers Exposed in Data Breach*, Infosecurity Mag. (Feb. 3, 2021), https://www.infosecurity-magazine.com/news/over-three-million-us-drivers/. Given the companies' poor track record of keeping data secure, it would be surprising for federal vehicle regulators to have written rules that rely on obscurity to maintain cybersecurity.

Finally, as noted in the recent Federal Trade Commission report, there is "no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data." Fed. Trade Comm'n, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* 31 (May 2021), https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf. What automakers *are* likely to do, absent legal requirements like those in the Right to Repair Act, is to further constrain the market for automotive service and repair. As an example, the FTC report cited LKQ Corp., a maker of aftermarket parts for automobiles, talking about the emerging practice of "VIN burning" in which automakers digitally couple parts to the vehicle's software and a specific vehicle's identification number (or VIN). With VIN burning, LKQ told the FTC, "a manufacturer can constrain a part to function with only a single car. Using the part on another vehicle would be blocked by the vehicle's embedded software." According to LKQ, VIN burning is already being used by General Motors and European luxury brands, while another auto manufacturer has implemented a software gateway on its vehicles, ostensibly to reduce the risk of vehicle exploitation, but which also blocks legitimate third party repairs on the vehicle. Fed. Trade Comm'n, *supra*, at 23.

Given the flaws of security through obscurity, this Court should reject plaintiff's invitation to

interpolate an obscurity mandate from generalized safety regulations and product recall authority. Federal regulators are unlikely to mandate a suboptimal practice, and a judicial precedent that cybersecurity regulations necessarily entail secrecy of data could have devastating consequences for the public.

III. The 2020 Right to Repair Law Enhances Consumer Protection, Competition, and Other Important Interests

The Right to Repair Act is exceptionally important to consumers, the economy, and society as a whole. The Act protects consumers' interest in repairing the cars that they own in order to maximize those cars' usefulness. Protection of this interest has a lengthy historical basis, and it serves as the foundation for a plethora of other public benefits including increased competition, consumer choice, lower prices, improved customer service, greater innovation, cultivation of small businesses, and a cleaner environment.

Consumers expect that, when they buy something, they are allowed to use it. *See* Aaron Perzanowski, *Consumer Perceptions of the Right to Repair*, 96 Ind. L.J. (forthcoming 2021) (manuscript at 23–24), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584377 (surveying consumers); 1 William Blackstone, *Commentaries on the Laws of England* *138 (1765) (describing rights of "free use, enjoyment, and disposal of all [one's] acquisitions"). From that premise comes "the lawful right of the owner to repair" purchased goods, namely "that right of care which every one may use to give duration to that which he owns." *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 365 U.S. 336, 346 (1961); *Wilson v. Simpson*, 50 U.S. (9 How.) 109, 123 (1850); *see also Kendall Co. v. Progressive Med. Tech., Inc.*, 85 F.3d 1570, 1573–74 (Fed. Cir. 1996) (reviewing cases).

By selling cars designed to be repairable only with telematics data that they control, the automobile manufacturers essentially give themselves a veto over the right to repair: The manufacturers can choose to monopolize the repair and aftermarket industries, or even refuse to permit repairs, forcing consumers to buy cars more often than necessary. *See* Daniel Hanley et al., Open Mkts., *Fixing America: Breaking Manufacturers' Aftermarket Monopoly and Restoring Consumers' Right to Repair* 10–11 (Apr. 2020). Indeed, vehicle and other product manufacturers have an extensive history of blocking competition in the repair industry starting with Ford in the early 20th century's use of nonstandard parts and tools. *See id.* at 6–7. Today, manufacturers stymie repair with a variety of additional strategies: gluing or welding casings together, or installing software to shut products off when aftermarket parts are installed, among other things. *See id.* at 6–14; Fed. Trade Comm'n, *supra*, at 17–24. The Right to Repair Act thus serves as an important consumer protection, ensuring that car owners are able to prolong the lifetimes of the vehicles that they bought and own without requiring permission from the manufacturer.

Protection of consumers' expectations of repair rights gives rise to a range of other benefits, chief among which is greater competition. It has long been recognized that restrictions on how consumers can use and repair their purchases can make the "smooth flow of commerce . . . sputter." *Impression Prods., Inc. v. Lexmark Int'l, Inc.*, 137 S. Ct. 1523, 1352 (2017); *see* Aaron Perzanowski & Jason Schultz, *The End of Ownership: Personal Property in the Digital Economy* 21 (2016). Judge Learned Hand recognized over 70 years ago that "reconditioning articles worn by use" could serve as an important check against monopoly market power. *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 425 (2d Cir. 1945). The Magnuson–Moss Warranty Act similarly is premised on the view that removing restrictions on repair rights, in the case of that law by prohibiting product warranty conditions limiting use of generic aftermarket parts or third-party repair services, will

"improve the adequacy of information available to consumers, prevent deception, and improve competition in the marketing of consumer products." Pub. L. No. 93-637, § 102(a), (c), 88 Stat. 2183, 2185–86 (1975) (codified at 15 U.S.C. §§ 2301–2312). The recent Federal Trade Commission study found as well that "repair restrictions may reduce consumers' options for obtaining spare parts and repair services in the aftermarket." Fed. Trade Comm'n, *supra*, at 16.

The usual effects of greater competition—lower prices and higher quality—are documented consequences of repair rights. For certain medical devices, for example, the FTC received evidence that independent repair services cost 25–50% less than the manufacturer's services. *See id.* at 40 (citing research by the International Association of Medical Equipment Remarketers and Services, Inc.). The Government Accountability Office estimated that reprocessing medical equipment saved hospitals between $200,000 and $1 million annually, and another study found that car owners can save about $300 a year by choosing independent repair shops. *See* U.S. Gen. Accounting Office, *GAO/HEHS-00-123, Single-Use Medical Devices: Little Available Evidence of Harm from Reuse, but Oversight Warranted* 19 (2000), http://www.gao.gov/new.items/he00123.pdf; Press Release, AutoMD, *Dealership or Repair Shop? AutoMD.com Debunks Top Five Myths* (May 17, 2010), https://www.automd.com/about-automd/articles/dealership-or-repair-shop/. Independent shops may also provide better customer service, as they are found in more places and can turn around repairs more quickly; the FTC's study found "scant rebuttal" to that proposition. Fed. Trade Comm'n, *supra*, at 39. By contrast, manufacturer-monopolized repairs are frequently criticized as slow and inconvenient, often requiring consumers to surrender their cars or essential devices for days or weeks to get them fixed. *Id.* (quoting Vermont State Senator Christopher A. Pearson); Ewan Spence, *Your Broken iPhone May Wait a Long Time to Be Fixed*, Forbes (Mar. 30, 2020), https://www.forbes.com/sites/ewanspence/2020/03/30/apple-iphone-repair-delay-right-

to-repair-coronavirus-covid19-social-distancing/ (documenting 4-week wait times for mobile phone repairs by manufacturer).

Unsurprisingly, the competition benefits of independent repair options mean that consumers are enthusiastically supportive of their right to repair. A forthcoming study finds that the "vast majority" of participants support a right to repair, and indeed about 50% of those with a damaged smartphone had sought independent repair services. Perzanowski, *supra*, at 23, 28. In the automotive industry particularly, an estimated 70% of the $392 billion aftermarket is held by independent shops. *See* John Lypen, *Editor's Report—Automotive Statistics—Independent Aftermarket*, Motor (May 2019), https://www.motor.com/magazine-summary/editors-report-may-2019/. The Right to Repair Act, as a ballot measure, passed by an overwhelming 75% of the vote in Massachusetts. *See* William Francis Galvin, Sec'y of the Commonwealth, Mass., *Return of Votes* 52 (Nov. 25, 2020), https://archives.lib.state.ma.us/handle/2452/839314. A prior automotive right to repair ballot measure in the state passed with 86% of the vote. *See* William Francis Galvin, Sec'y of the Commonwealth, Mass., *Return of Votes* 55 (Nov. 28, 2012), https://archives.lib.state.ma.us/handle/2452/200393.

A right to repair has further second-order benefits as well. Valuable consumer innovation can arise when consumers of technological devices have the ability to repair and modify them. *See* Eric von Hippel, *Democratizing Innovation* 72–74 (2005). The importance of this consumer-driven innovation was made clear recently when a hospital inundated with COVID-19 patients used 3D-printing technology to make replacement ventilator parts—despite the ventilator manufacturer's reported unwillingness to sanction the hospital's repairs. *See* Jay Peters, *Volunteers Produce 3D-Printed Valves for Life-Saving Coronavirus Treatments*, The Verge (Mar. 17, 2020), https://www.theverge.com/2020/3/17/21184308/coronavirus-italy-medical-3d-print-valves-treatments.

See generally Yu Ying Clarrisa Choong et al., *The Global Rise of 3D Printing During the COVID-19 Pandemic*, 5 Nature Reviews Materials 637 (Sept. 1, 2020), https://www.nature.com/articles/s41578-020-00234-3.

Repair rights also strengthen small businesses, as independent repair shops are often small firms. *See* Fed. Trade Comm'n, *supra*, at 3–4. In 2015, the average number of technicians at an independent car repair shop was between 3 and 4, and "small operators dominate" the smartphone repair industry, with the largest firms making up just 10% of the market. *See Average Number of Technicians at Independent Repair Shops Up*, Automotive Res. (Jan. 28, 2016), https://www.automotiveresearch.com/insights/average-number-of-technicians-increased-at-independent-repair-shops; Sarah Kahn, *IbisWorld Report OD5802*, *Cell Phone Repair in the US* 18 (May 2014). And a robust repair economy protects the environment by avoiding product waste, when independent repair shops can fix devices that the manufacturer would prefer consumers to throw away. *See* Fed. Trade Comm'n, *supra*, at 41–42; Nathan Proctor, U.S. PIRG Educ. Fund, *The Fix Is In: How Our Smartphones Get Fixed, Why It's Harder Than It Should Be, and Why That Matters* 4 (Mar. 2020), https://uspirg.org/sites/pirg/files/reports/The-Fix-Is-In/The_Fix_Is_In_March2020_USPEF.pdf.

These many benefits that arise from a robust right to repair are the reason that laws like the Right to Repair Act are being debated in numerous states, not just with respect to cars but also for other consumer products. *See* Nathan Proctor, *Half of U.S. States Looking to Give Americans the Right to Repair*, U.S. PIRG (Mar. 10, 2021), https://uspirg.org/blogs/blog/usp/half-us-states-looking-give-americans-right-repair. Plaintiff's efforts to deem such laws federally preempted will thus have potentially widespread effects on the rights and interests of Americans, far beyond either the Commonwealth of Massachusetts and the technology of vehicle telematics.

CONCLUSION

For the foregoing reasons, this Court should hold that the Right to Repair Act is not preempted as a matter of law.

Respectfully submitted,

Dated: June 7, 2021

/s/ Christoper T. Bavitz
Christopher T. Bavitz (BBO #672200)
Cyberlaw Clinic, Harvard Law School
1585 Massachusetts Ave.
Cambridge, MA 02138
Tel: (617) 384-9125
Email: cbavitz@law.harvard.edu

Counsel for Amici Curiae