Journal of Law and Mobility

Volume 2020

2020

Who Gets to Operate on Herbie? Right to Repair Legislation in the Context of Automated Vehicles

Jennifer J. Huseby
University of Michigan Law School

https://doi.org/10.36635/jlm.2020.who

WHO GETS TO OPERATE ON HERBIE? RIGHT TO REPAIR LEGISLATION IN THE CONTEXT OF AUTOMATED VEHICLES

JENNIFER J. HUSEBY†

Cite as: Jennifer J. Huseby, Note, *Who Gets to Operate on Herbie? Right to Repair Legislation in the Context of Automated Vehicles*, 2020 J.L. & MOB. 41.
This manuscript may be accessed online at https://futurist.law.umich.edu/ and at https://repository.law.umich.edu/jlm/.

ABSTRACT

You bought it, you own it, but do you have the right to repair it? As right-to-repair remains a hot topic in the context of consumer electronics such as smartphones, one must consider the ramifications it may have for the automated vehicle ("AV") industry. As the backdrop for one of the first legislative victories for right-to-repair, the automobile industry has continued to push for the expansion of right-to-repair to cover increased access to telematics and exceptions to proprietary software controls. However, as we revisit the issue for more highly connected and automated vehicles, it is important to assess the unique considerations of the AV sector before we can transpose previously learned lessons into a new, nearly unpredictable context.

As such, this article examines a possible framework that addresses the technical and privacy concerns that uniquely arise when applying right-to-repair legislation to AVs. By attempting to predict on how previously learned lessons may influence action going forward, this article hopes to influence the right-to-repair discourse that will arise between

† J.D. Candidate, University of Michigan Law School (2021); B.A. Korea University (2017). This paper was written as a final project for the course offering of Legal Issues Surrounding Autonomous Vehicles at the University of Michigan Law School during the Winter 2020 semester, taught by Emily Frascaroli. The author may be contacted at jenjhuseby@gmail.com.

manufacturers, consumers, and independent repair technicians for AVs.

TABLE OF CONTENTS

INTRODUCTION

"You bought it, you own it,"[1] but the question is: do you have the right to repair it? Many of us may have tried a frantic Google search for "how to replace screen cheap" after a nasty coupling between concrete and iPhone. Some of us may have even ventured to a local independent repair technician to get that spider webbed screen replaced. Yet behind this seemingly simple sequence of events lies a legal and regulatory battleground around "right-to-repair" legislation, involving a clash between manufacturers' desire to protect their intellectual property and consumers who seek complete ownership of their devices. And as companies increasingly invest in the research and development of automated vehicles ("AVs"), the question now turns to whether people should be free to peek under "Herbie's" hood and repair their own AVs as well (or at least, have access to a free market with alternative independent repair technicians).

AVs have the potential to revolutionize transportation systems by increasing safety, providing critical mobility access, and creating greater efficiency and fuel savings.[2] However, initial costs and maintenance charges serve as exceedingly high barriers to mass-market implementation and penetration.[3] Although the price tag on key technology components such as

1. Corynne McSherry & Parker Higgins, *You Bought it, You Own It: Supreme Court Victory for Common Sense and Owners' Rights*, ELECTRONIC FRONTIER FOUNDATION (Mar. 19, 2013), https://www.eff.org/deeplinks/2013/03/you-bought-it-you-own-it-supreme-court-victory-common-sense-and-owners-rights.

2. Daniel J. Fagnant & Kara Kockelman, *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations*, 77 TRANSP. RES. PART A: POL'Y & PRAC. 167, 169-75 (2015).

3. *See id.* at 175-78, *see also* Russ Mitchell, *Lidar Costs $75,000 Per Car. If the Price Doesn't Drop to a Few Hundred Bucks, Driverless Cars Won't Go Mass Market*, L.A. TIMES (Dec. 11, 2017), https://www.latimes.com/business/la-fi-hy-ouster-lidar-

LIDAR are decreasing incrementally, figures still cite that fully autonomous technology adds up to an extra $100,000 to the price of an individual vehicle.[4] Providing more affordable repair and maintenance options through independent repair shops could be the key to providing cheaper access to AVs, which in turn may prove necessary for mass-market level implementations that could fully take advantage of their benefits.

On the other hand, it is understandable to feel cautious of entrusting AV repair to those that are not original equipment manufacturers ("OEMs"). Right-to-repair, which allows for consumers and third-party vendors to open up and repair their products, is promising in the context of phones or non-AV automobiles. However, opening up Herbie's hood conjures images of complex circuitry and elaborate schematics that local mechanics may not have seen before. More importantly, AVs involve increased security and privacy concerns when compared to traditional vehicles.

The intense integration of software in AVs means that any potential vulnerabilities in the vehicle's security may result in physical, potentially catastrophic crashes.[5] Given the potential for malicious actors to take advantage of these vulnerabilities, the question not only becomes whether we should entrust the safety of the driver and the public to tinkerers, but also whether it is prudent to do so at the expense of the investment rights and potential reputational damage of OEMs. Finally, current intellectual property statutes such as the Digital Millennium Copyright Act ("DMCA"), which criminalizes the circumvention of "access controls" such as the OEM's protective software,[6] may even preempt states from enacting such right to repair laws.[7]

This article examines a possible framework to address the technical and privacy concerns that uniquely arise when applying right-to-repair legislation to AVs. To do so, this article attempts to predict how previously learned lessons may influence right-to-repair issues that may arise for AVs. Part I explains the right-to-repair movement, its key stakeholders, and the legal and factual development of such legislation in the United States. In Part

---

20171211-htmlstory.html.

4. Lance Eliot, *LIDAR Game of Thrones for Driverless Cars, There Will Be Winners and There Will Be Losers*, FORBES (Apr. 16, 2019), https://www.forbes.com/sites/lanceeliot/2019/04/16/lidar-game-of-thrones-for-driverless-cars-there-will-be-winners-and-there-will-be-losers/?sh=3539c1f91f13.

5. *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (Jul. 21, 2015) https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

6. Access controls refer generally to copyright owners' exertion of control over consumers' access to the contents of their works. *See* JESSICA D. LITMAN, DIGITAL COPYRIGHT 83 (2nd ed. Amherst, N.Y.: Prometheus Books, 2006).

7. 17 U.S.C.A. § 1201.

II, this article discusses the common arguments marshaled for and against right-to-repair legislation, mostly predicated on freedom and security concerns. In Part III, this article proposes a regulatory right-to-repair framework that targets the unique concerns of AVs specifically, explaining the necessity of preserving the privacy of consumer's data and acknowledging the need for highly qualified technical skill when working on these vehicles.

PART I: THE RIGHT-TO-REPAIR "MY STUFF"

Right-to-repair is the embodiment of the idea of complete ownership. In other words if you own it, you "should be able to open, hack, repair, upgrade, or tie bells on" on it in whatever way you choose.[8] Chief among its leaders is the Repair Association, which includes notable industry organizations and consumer-rights groups such as the Electronic Frontier Foundation ("EFF"),[9] iFixit,[10] and other players that are similarly impassioned and involved in advocating for the repair and reuse of technology.[11] The movement encompasses a surprisingly broad array of industry interests, including medical device repair and maintenance, automobiles, agriculture and farming, and consumer electronics spaces.[12]

There is much more to the right-to-repair movement than a want of ownership and control over one's purchase. Concerns of efficiency and timeliness are also commonly cited by consumers as a reason to support right-to-repair. For example, American farmers have taken to hacking their John Deere tractors with Ukrainian firmware off of the black market.[13] They

8. *We Have the Right to Repair Everything We Own*, IFIXIT https://www.ifixit.com/Right-to-Repair/Intro (last visited Aug. 12, 2020).

9. EFF is a nonprofit organization dedicated to defending civil liberties in the digital frontier, with a chief focus on protecting access to developing technology. Some notable legal victories include advocating for exemptions to Section 1201 of the DMCA, so as to allow legal "break[ing]" of digital access controls to repair and otherwise use technology more freely. *See About EFF*, EFF, https://www.eff.org/about; *see also* Mitch Stoltz, *New Exemptions to DMCA Section 1201 Are Welcome, But Don't Go Far Enough*, EFF (Oct. 26, 2018) https://www.eff.org/deeplinks/2018/10/new-exemptions-dmca-section-1201-are-welcome-dont-go-far-enough.

10. iFixit, "the Free Repair Manual" is a wiki-based site and community dedicated towards teaching "the world to fix every single thing" by allowing users to share technical knowledge through provisions and edits of repair manuals. *See, e.g.*, *The Repair Revolution*, IFIXIT, https://www.ifixit.com/Right-to-Repair (last visited Aug. 12, 2020); *Who we are*, IFIXIT, https://www.ifixit.com/Info/background (last visited Aug. 12, 2020).

11. *See About Us: Members*, REPAIR.ORG, https://repair.org/members-1/ (last visited Aug. 12, 2020).

12. *See id.*

13. Jason Koebler, *Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware*, VICE (Mar. 21, 2017) https://www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware.

do this because John Deere software has made it impossible to perform unauthorized repairs on their equipment,[14] and the farmers "don't have time to wait for a dealership employee to show up and fix it,"[15] due to the nature of farm work. Waiting for dealerships or manufacturers to respond to repair requests could end up costing farmers crucial time during harvesting periods, ultimately hurting their livelihoods.[16]

Right-to-repair movements have been successful in persuading manufacturer side institutions such as the Equipment Dealers Association to make concessions. These concessions include agreeing to provide repair manuals, product guides, diagnostic service tools, and on-board diagnostics to farmers by 2021.[17] Yet even this agreement contained carveouts allowing manufacturers to continue using proprietary software locks designed to prevent repair.[18] Unsurprisingly, this type of software lock is an important puzzle piece in right-to-repair – and it isn't just limited to tractors.

Microprocessors and accompanying software are now ubiquitous in our coffee machines, cars, CPAP machines, ventilators and more – and while the complexity hasn't necessarily deterred the ability of independent repair technicians to fix the product, Digital Rights Management ("DRM") software locks placed by the manufacturer make the problem an issue of authorized access. DRM is a euphemism for technologies implemented by IP holders and manufacturers that are designed to control how, where and when their consumers use their products and content after purchase.[19] This type of software serves as a gatekeeper to enforce any restrictions or limitations demanded by manufacturers, and can do things like restrict your iTunes purchases to Apple products, or prevent you from using your DVR to record your favorite show if the copyright holder objects.[20]

---

14. JOHN DEERE, *License Agreement for John Deere Embedded Software* 1, https://www.deere.com/assets/pdfs/common/privacy-and-data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf (last accessed Oct. 23, 2020) (illustrating how software related end user license agreements restrict unauthorized repair).

15. *See* KOEBLER, *supra* note 13.

16. Kyle Wiens & Elizabeth Chamberlain, *John Deere Just Swindled Farmers out of Their Right to Repair*, WIRED (Sep. 19, 2018) https://www.wired.com/story/john-deere-farmers-right-to-repair/.

17. Jason Koebler, *Farmer Lobbying Group Sells Out Farmers, Helps Enshrine John Deere's Tractor Repair Monopoly*, VICE (Sep 11, 2018) https://www.vice.com/en/article/kz5qgw/california-farm-bureau-john-deere-tractor-hacking-right-to-repair?

18. *Id.*

19. AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY 121 (2016).

20. *Id.* at 135. *See also* Eric Bangeman, *DirecTV DVR Clampdown: A Sober Reminder of DRM Suckitude*, ARS TECHNICA, March 20, 2008, https://arstechnica.com/uncategorized/2008/03/directv-dvr-clampdown-a-sober-reminder-of-drm-suckitude/ (last visited Aug. 12, 2020).

Unfettered ownership for the consumer sounds amazing. Ownership free from DRM encourages innovation and efficiency in repair, because this "freedom to tinker" lets individuals contribute to technologies in creative ways that the OEM does not (or cannot).[21] Yet it is not surprising that manufacturers would want to limit the scope of after-sale repairs and maintenance for purchasers. After all, some estimate that repair business may account for up to three percent of the United States' economy.[22] After-sale repair and maintenance markets are a lucrative revenue steam that original manufacturers are incentivized to capitalize on; and this is not to mention the safety and security concerns that may arise from granting such unfettered access to software controls and diagnostics. To that end, many manufacturers have taken the road towards cementing a virtual repair monopoly, by restricting access to repair manuals and replacement parts, using DRM software to wall off potential do-it-yourselfers from attempting to fix their products, and lobbying lawmakers to oppose legislation that would protect and expand access to repair capital.[23]

History and Developments in Right-to-Repair Legislation

Despite being touted by progressive politicians,[24] right-to-repair is more culturally conservative than we would expect.[25] The United States "started as a nation of tinkerers," building new ways to disrupt existing industries

---

21. PERZANOWSKI & SHULTZ, *supra* note 19, at 135; *see also* Eric Von Hippel, *Democratizing Innovation* 121 – 124 (Cambridge, MA: MIT Press, 2005) http://web.mit.edu/evhippel/www/democ1.htm (last visited Oct. 23, 2020) (illustrating the inefficiencies that result when we avoid user-centered innovation systems that model that work on democratizing innovation and creativity).

22. *See also* IFIXIT (Oct. 25, 2018), https://ifixit.org/blog/11951/1201-copyright-final-rule/ (stating that "repair jobs represent 3% of overall employment" in the American economy).

23. Jason Koebler, *Appliance Companies are Lobbying to Protect Their DRM-Fueled Repair Monopolies*, VICE (Apr. 25, 2018) https://www.vice.com/en/article/vbxk3b/appliance-companies-are-lobbying-against-right-to-repair. This article illustrates the efforts of electronics manufacturers such as Dyson, LG, and Wahl to oppose now stagnant Illinois Bill HB 4747, which would have required such electronics manufacturers to:

> "sell replacement parts and tools, [allow] independent repair professionals and consumers to bypass software locks that are strictly put in place to prevent unauthorized repair, and would require manufacturers to make available the same repair diagnostic tools and diagrams to the general public."

24. *See, e.g.*, *Warren and Sanders Say We Need a "Right to Repair" Tractors. Here's Why That's Important*, IN THESE TIMES (Aug. 1, 2019) http://inthesetimes.com/article/21952/right-to-repair-technology-Apple-manufacturing.

25. Louis Rossman, *What is Right to Repair? An Introduction for Curious People*, YOUTUBE (Mar. 4, 2020), https://www.youtube.com/watch?v=Npd_xDuNi9k.

through experimentation and innovation.[26] Despite this, "tinkering" is quickly becoming discouraged as manufacturers seek new ways to protect and restrict the use of their intellectual property after-purchase, and as concerns of safety and cybersecurity grow increasingly poignant.

The history of right-to-repair in the automotive industry begins in Massachusetts. The Motor Vehicle Owner's Right to Repair Act was a landmark achievement in the automotive space, eventually paving the way for a national solution between independent repair technicians and OEMs[27]. Not content with the initial passage of the law in 2012, pro-repair rights groups were further able to pass a ballot initiative that would allow vehicle owners and repair technicians access to the same diagnostic and repair information that before, had only been available to manufacturers and manufacturer-authorized facilities.[28] Massachusetts voters overrode the car companies with 74% of voters supporting this right-to-repair ballot measure in November 2012.[29] This wildly successful initial campaign in Massachusetts was spearheaded by the Auto Care Association ("Auto Care"), a national trade organization comprised of 3,000 members representing more than 150,000 independent auto care businesses.[30]

Right-to-repair continues to be wildly popular in Massachusetts, and the movement very recently saw a win in the 2020 election season, in which an amendment to allow vehicle owners and independent mechanics access to telematics passed with 75 percent approval.[31] Telematics are the data that is

---

26. *See, e.g.*, ALEC FOEGE, THE TINKERERS: THE AMATEURS, DIYERS, AND INVENTORS WHO MAKE AMERICA GREAT (2013); Daniel J. Kevles, *The U.S. Started as a Nation of Tinkerers*, SCIENTIFIC AMERICAN (Dec. 12, 2015) https://www.scientificamerican.com/article/the-u-s-started-as-a-nation-of-tinkerers/.

27. Motor Vehicle Owners Right to Repair Act of 2011, H.R. 1449, 112th Cong. (2011-2012), https://www.congress.gov/bill/112th-congress/house-bill/1449?s=1&r=17; *see* Leah Chan Grinvald and Ofer Tur-Sinai, *Intellectual Property Law and the Right to Repair*, 88 FORDHAM L. REV. 63, 72 (2019).

28. Sec. of the Commonwealth of Mass., *Statewide Ballot Questions — Statistics by Year: 1919 – 2018*, https://www.sec.state.ma.us/ele/elebalm/balmresults.html #year2012 (showing 74% of voters in support of Question 1, an initiative petition for a law on Availability of Motor Vehicle Repair Information).

29. *Id.*, *see also* Erine Smith, *Years After Success, Massachusetts Right to Repair Coalition Re-Forms to Close Loophole* (Feb. 6, 2019), https://associationsnow.com/2019/02/massachusetts-right-repair-coalition-re-forms-close-loophole/ (stating that after the success in 2012, the Right to Repair Coalition is still fighting in 2020 to close the telematics loophole by advocating for an update to the law).

30. *Right to Repair*, AUTO CARE ASS'N, https://www.autocare.org/government-affairs/issues/right-to-repair/.

31. *Mass. Election Results*, WCVB TV (Nov. 3, 2020), https://elections.ap.org/WCVB/results/2020-11-03/state/MA/race/I/raceid/24900; *see also* Adi Robertson, *Massachusetts passes 'right to repair' law to open up car data*, THEVERGE (Nov. 4, 2020) https://www.theverge.com/2020/11/4/21549129/ massachusetts-right-to-repair-question-1-wireless-car-data-passes.

transmitted wirelessly from the vehicle to the manufacturer, and can include data such as driving behavior, GPS location, and repair and maintenance data.[32] Amidst projections that 87% of new vehicles in the United States would transmit such data,[33] these results were a crucial win in the fight for legislation that would allow consumers to have more control over who has access to this data, and allow members of the auto care industry to use this data to assist with maintenance and repair.

In brief, the Massachusetts Right to Repair Act granted car owners – thus including the average consumer, and independent repair shops – access to the manuals and diagnostic software that licensed dealerships had, thus vastly facilitating independent repair efforts and expanding the range of repair options consumers would have available. This was buttressed by the subsequent agreement with the Association of Global Automakers, which gave mechanics similar rights.[34]

Inspired by the successes in Massachusetts's automobile repair industry, the right-to-repair movement appeared to gain steam across the nation and across various commercial fields.[35] Its popularity led over twenty states to introduce some form of right-to-repair legislation that draws upon model legislation drafted by the Repair Association itself.[36] Largely, such legislation would expand consumer access to the repair manuals, tools, and replacement parts that they need to fix their electronic equipment.[37] Yet despite initial steam, many of these efforts, outside of Massachusetts, seem to have stalled since their inception.[38]

Right-to-Repair in the Courts

Repair doctrine is not a foreign concept in the courts. Intellectual property law has traditionally interpreted ownership rights as extending far past mere physical possession,[39] and repair rights are no exception. Notably, the right-

32. *Access to and Control of Vehicle Data*, AUTO CARE ASS'N, https://www.autocare.org/government-affairs/issues/telematics/.

33. *Car Data Factsheet*, AUTO CARE ASS'N, https://www.autocare.org/uploadedfiles/autocareorg/government_affairs/issues/resources/consumer_cardatafactsheet.pdf.

34. Christopher Jensen, *Carmakers to Share Repair Data*, N.Y. TIMES (Jan. 31, 2014), https://www.nytimes.com/2014/02/02/automobiles/carmakers-to-share-repair-data.html.

35. *See* Repairable Products Make Good Sense, IFIXIT, https://www.ifixit.com/Right-to-Repair/Repairable-Products (last visited Nov. 10, 2020) (currently, right-to-repair is often discussed in the context of consumer electronics such as smartphones).

36. REPAIR ASS'N, MODEL STATE RIGHT-TO-REPAIR LAW, (July 24, 2018), https://repair.org/s/Right-to-repair-Model-state-law-7-24-18.docx.

37. *Id.*

38. Grinvald & Tur-Sinai, *supra* note 27 at 72 – 73.

39. *See, e.g.*, Impression Prods. v. Lexmark Int'l., Inc., 137 S. Ct. 1523 (2017) (for

to-repair has enjoyed protection as an extension of the exhaustion principle in patent law.[40] Dubbed the principle of permissible repair, courts recognize that one who is lawfully using a patented item has the lawful right to preserve and maintain the item in a usable and functional status by repairing the item.[41] Such permissible repair allows replacements of the item's component parts, as long as the replacement does not amount to a reconstruction. Indeed, "[t]he Supreme Court has taken an expansive view of the conduct that constitutes permissible repair of a patented combination of unpatented elements."[42]

After-sale market businesses that maintain, repair, customize, refurbish or otherwise resell products have long relied on the exhaustion principle to balance the competing interests of the patent owner's exclusive property rights, the consumer's rights to resell and otherwise repair or improve their purchases, and public interest to prevent unfair competition.[43] Interestingly, broad constructions of the principle of permissible repair are seen especially in the context of medical device maintenance cases,[44] even though one would expect a higher consideration of the patent owner's rights because of public interest in maintaining high quality repair standards for the sake of medical safety.

However, there is an increased trend towards separating ownership rights from purchase. We are already in an age that deemphasizes ownership. The insurgence of the right-to-repair movement can be traced to the development of end-user license agreements ("EULA").[45] In a nutshell, EULAs are legal contracts, typically involving software, entered into by copyright owners (generally software developers) and consumers that restrict the consumers from redistributing the software or otherwise engaging in use unwanted by

---

example, the first sale doctrine in copyright has long been recognized and reaffirmed by courts and limits the extent to which owners of intellectual property can control their product or service after an initial sale).

40. *See id.* (rooted in common law, the exhaustion principle is the notion that a holder of intellectually property rights relinquishes, or "exhausts" their control over a product once it sells or otherwise transfers title of that property to someone else).

41. Aro Mfg. Co. v. Convertible Top Replacement Co., 365 U.S. 336 (1961).

42. Sage Products, Inc. v. Devon Indus., Inc., 45 F.3d 1575, 1578 (Fed. Cir. 1995).

43. Brief *Amici Curiae* of Auto Care Ass'n and Int'l Imaging Tech. Council in Support of the Petitioner at 3, Impression Products, Inc. v. Lexmark International, Inc., 137 S. Ct. 1523 (2017) (No. 15-1189) at 3, https://www.scotusblog.com/wp-content/uploads/2017/02/15-1189_amicus_pet_auto_care_assoc.pdf.

44. *See* § 11:59. Right-to-repair, 2 ANNOTATED PATENT DIGEST § 11:59; *see also* Kendall Co. v. Progressive Med. Tech., Inc., 85 F.3d 1570 (Fed. Cir. 1996) (finding that when patent assignee sold its patented medical device for applying compressive pressure to patients' limbs, assignee granted customers implied license to use device for its useful life, and implied license included right-to-repair patented article and necessarily to purchase repair parts from others; right-to-repair was implied as matter of law).

45. PERZANOWSKI & SCHULTZ, *supra* note 19 at 2.

the owners—and they are now near-ubiquitous. Taken from software licensing agreements, consumers now see EULAs daily in smartphone applications, and platforms like Netflix and Spotify.[46] The world is transforming towards a "sharing economy," shown most clearly in the expansion of these temporary-access business models.[47] Needless to say, the broad coverage of the repair doctrine may depend on whether jurisprudence around EULAs going forward will continue to favor expansive interpretations of ownership or will instead trend towards emphasizing the original manufacturer's control over their after-sale products.[48]

PART II: THE BATTLE BETWEEN FREEDOM AND SECURITY INTERESTS

The traditional arguments lobbying for and against right-to-repair legislation largely follow an ideological push and pull cleavage between freedom and security interests. Consumers and independent repair technicians will identify with those arguments that highlight consumer freedom to fix the products that they own, or at least have the option to have their products fixed by whomever they choose. Conversely, manufacturers will rightly point out the various security vulnerabilities that may arise in accommodating the bypass and availability requests of the general public. After all, the primary purpose of controls like DRM software is to protect the integrity of a product, its software, and the information that it collects.

The following sections will assess traditional arguments on both sides, while transposing them onto the AV context. In doing so, some key factors to consider are the unique safety and security risks that AVs would be characteristically exposed to, the new nature of the industry and its infrastructure, and the particular relevance of copyright laws and the DMCA due to the high integration of software in the vehicles themselves.

Consumer Freedom Based Interests: Efficiency & Access

A commonly posed question by proponents of right to repair is: "would you buy a car if it was illegal to replace the tires?"[49] The question is commonly cited because of how persuasive it is—after all, most people are likely to answer: "no." Repairing a broken chain on a bicycle, restoring classic cars, and taking apart gadgets is something that feels inherent in one's ownership of a product. Any consumer would balk at having to spend

46. *See id.* at 169.

47. *Id.* at 170.

48. In fact, recent case law would suggest the latter, erecting more barriers for right to repair going forward. *See, e.g.*, Vernor v. Autodesk, Inc., 621 F.3d 1102, 1111 (9th Cir. 2010) (holding that computer software customer was licensee of its copy rather than owner, and thus was not entitled to invoke first sale doctrine or essential step defense).

49. IFIXIT, supra note 8.

exorbitant sums (or even potentially facing legal action) just to replace the side front wheel of their car—even if that car was a sentient Volkswagen Beetle. Yet this is precisely the issue that faces owners of increasingly complex vehicles, and the necessity of right-to-repair advocacy and legislation will continue to rise as boundaries around ownership are pushed to unprecedented degrees.[50]

Of course, some arguments circling efficiency reasons may prove less or more persuasive when transposed on to the context of AVs. As an example, electronic waste ("e-waste") and environmental conservation are widely cited reasons to support right-to-repair and the recycling or upcycling of consumer electronics, such as smartphones.[51] Notably, such e-waste accounted for waste streams of over 50 million tons in 2018 and is estimated to reach 120 million tons by 2050.[52] However, this argument is not as persuasive in the AV context, as such vehicles are extremely expensive. Here, consumers are less likely to engage in "wasteful" spending habits such as simply purchasing a new car in response to a defective part. This contrasts highly with "buy new, buy now" marketing models that companies such as Apple have been accused of following, through planned obsolescence type tactics such as engineering iPhone batteries that die out within a matter of years, and by patching handsets with software intended to slow down older generation phones.[53]

At the same time, some consumer freedom arguments prove uniquely persuasive for automated vehicles. One such argument is that because right-to-repair laws allow for a greater number of independent repair technicians to service and maintain vehicles, repairs will cost less and conclude faster – thus allowing greater access to mass-market consumers. There are delays and undue expenses in dealer-monopolized repair schemes, and dealers may be unequipped to absorb the capacity of small, minor fixes on a commercial

---

50. *See, e.g.*, Neil Gladstone, *We Need Right-to-Repair Laws Now More Than Ever*, DIGITAL TRENDS (July 18, 2020) https://www.digitaltrends.com/features/right-to-repair-legislation-now-more-than-ever/ (detailing the story of Youtuber Rich Benoit and his channel's quest to "salvage and reverse engineer trashed Teslas" after experiencing first-hand frustration at how difficult the vehicles are to fix, even for minor, routine issues such as a ripped tire).

51. As an example, electronic waste ("e-waste") and environmental conservation reasons are widely cited as a reason to support right-to-repair and recycling or upcycling of consumer electronics, such as smartphones. *See, e.g.* Jennifer Huseby, *Cars, Smartphones and Waste: Fighting for the Right to Repair in 2019*, MTLR BLOG (Nov. 20, 2019) https://mttlr.org/2019/11/cars-smartphones-and-waste-fighting-for-the-right-to-repair-in-2019/.

52. WORLD ECONOMIC FORUM, A NEW CIRCULAR VISION FOR ELECTRONICS: TIME FOR A GLOBAL REBOOT, 10 (2019).

53. Jen Kirby, *Apple Admitted It's Slowing Down Certain iPhones*, VOX (Dec. 28, 2017, 5:00 P.M.), https://www.vox.com/2017/12/22/16807056/apple-slow-iphone-batteries.

scale.

Wider access to repairs can be the difference between life and death. The FDA stated in 2018 that "the continued availability of third party entities to service and repair medical devices is critical to the functioning of the U.S. healthcare system."[54] This is largely because healthcare establishments need cost-effective alternatives to simply purchasing new equipment.[55] For example, Stephen Grimes, a managing partner at Strategic Healthcare Technology Associates LLC, posited that manufacturers may charge between ten and fifteen percent of the cost of the medical device for maintenance services, while in-house or service organization repairs could offer such services for four to six percent.[56]

This need was highlighted most starkly during the current COVID-19 pandemic. As medical workers grew increasingly strapped for functioning ventilators, hospitals have tried to repair the ventilators that they do have to combat the shortage.[57] According to Gay Gordon-Byrne, the executive director of Repair.org, some "on-site biomedical technicians can fix a ventilator in hours and return it to service more quickly than anyone else. If they can't get the info they need to fix and restore to use—a whole lot of very sick people won't have essential care."[58] Yet in response to this, manufacturers have threatened to sue independent databases of repair manuals.[59] Importantly, the medical device examples show us that even in life or death situations, independent repair technicians can be relied upon and trusted, and that sometimes, they are the only feasible alternative.

Manufacturer Concerns: Safety & Security Based Interests

Automated vehicles offer a unique challenge to right-to-repair supporters in that they combine traditional cybersecurity concerns with real physical

---

54. FDA, FDA REPORT ON THE QUALITY, SAFETY, AND EFFECTIVENESS OF SERVICING OF MEDICAL DEVICES: IN ACCORDANCE WITH SECTION 710 OF THE FOOD AND DRUG ADMINISTRATION REAUTHORIZATION ACT OF 2017 (FDARA) i (May 2018).

55. *Id.* at 10.

56. Agam Shah, *Who Has a Right to Repair Your Farm or Medical Tools?*, ASME (Apr. 16, 2019) https://www.asme.org/topics-resources/content/has-right-repair-farm-medical-tools.

57. Jason Koebler, *Hospitals Need to Repair Ventilators. Manufacturers Are Making That Impossible*, VICE (Mar. 18, 2020) https://www.vice.com/en_us/article/wxekgx/hospitals-need-to-repair-ventilators-manufacturers-are-making-that-impossible. *See, e.g.*, Jerri-Lynn Scofield, *Right to Repair and Ventilators: Saving COVID-19 Patients*, NAKED CAPITALISM (Apr. 5, 2020) https://www.nakedcapitalism.com/2020/04/right-to-repair-and-ventilators-saving-covid-19-patients.html; Cory Doctorow, *Right to Repair in Times of Pandemic*, EFF (Mar. 19, 2020) https://www.eff.org/deeplinks/2020/03/right-repair-times-pandemic.

58. Koebler, *supra* note 56.

59. *E.g.*, *id.*

danger to the purchaser's safety. After all, the modern-day vehicle is extremely complex—it is essentially a "computer on wheels."[60] Modern vehicles may contain an impressive amount of software with over 100 million lines of code, which operate microprocessor-based electronic control units ("ECUs") that manipulate anywhere from minor to crucial functions such as the wipers, to the brakes and even steering.[61] Predictably, the increasing complexity arising from connectivity and semi-autonomous capabilities brings vulnerabilities that expose the vehicle further just as if it were a computer – but with physical, potentially catastrophic effects.[62]

Nowhere is this more apparent than in the potential exploitation of on-board diagnostic ("OBD-II") systems. The OBD-II is an innocent looking 16-pin connector port, located in the driver-side footwell of a car,[63] yet it is essentially an on-board computer that monitors an incredible amount of data about the vehicle including emissions, mileage, speed and more.[64] These innocuous seeming ports have been mandated on new American cars since 1996, as part of an effort to direct OEMs to make diagnostic tools and information available to independent repair technicians and the general public.[65]

The issue is that access to OBD technical information renders vehicles extremely vulnerable to outside attacks. Famous car hackers Chris Valasek and Charlie Miller have spent years demonstrating the concerns over cybersecurity in our vehicles, highlighting remote attacks that can result in hijacking the physical control over a car as the most pressing area of concern.[66] Notably, Valasek and Miller were able to demonstrate how hackers can remotely steal control of a moving vehicle on the highway in a zero-day exploit—a vulnerability that is taken advantage of by attackers

60. DAN KLINEDINST & CHRISTOPHER KING, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY, ON BOARD DIAGNOSTICS: RISKS AND VULNERABILITIES OF THE CONNECTED VEHICLE v (2016) https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf.

61. Robert N. Charette, *This Car Runs on Code*, IEEE SPECTRUM (Feb. 1, 2009) https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code; *see also* KLINEDINST & KING, *supra* note 59 at 1.

62. *See* KLINEDINST & KING, *supra* note 59, at 1.

63. *Id.*

64. Ryan Dube, *What is the OBD-II Port and What Is It Used For?*, MAKEUSEOF (Dec. 21, 2018) https://www.makeuseof.com/tag/obd-ii-port-used/#:~:text=OBD%2DII%20is%20an%20on,under%20the%20driver%27s%20side%20dash.

65. *See* 40 CFR § 86.1806-05(a)(1) (mandating that "all light-duty vehicles, light-duty trucks and compete heavy-duty vehicles . . . must be equipped with an onboard diagnostic (OBD) system capable of monitoring all emission-related powertrain systems or components during the applicable useful life of the vehicle.").

66. Lindsey O'Donnell, *Chris Valasek and Charlie Miller: How to Secure Autonomous Vehicles*, THREATPOST (Aug. 10, 2018) https://threatpost.com/chris-valasek-and-charlie-miller-how-to-secure-autonomous-vehicles/134937/.

before developers have an opportunity to respond to it (hence the term "zero-day").[67]

Just as in the medical device context, manufacturers will also likely cite concerns about the quality of servicing provided by third party technicians as a reason to oppose right-to-repair legislation.[68] Components are so highly integrated in electronics and equipment that they are difficult for owners to fix – which starts to beg the question whether we should be letting them try. The integration of more technology into devices and vehicles means that repair shops may not have the skillset or the rights to work on newer products. For example, even for a simple tire repair, you need to calibrate a software-controlled tire pressure sensor – a stretch more complicated than slapping on an aftermarket tire on a tractor.

However, it is important to note that for medical devices, the FDA has largely concluded that third party repairs are not dangerous and provide "high quality, safe, and effective servicing of medical devices."[69] Industry leaders report that this is especially so where the organization has established quality systems, ensured that adequate and appropriate training was in place, and where validated parts are being used for repair and servicing activities.[70]

Still, this infrastructure takes time to build, especially for radically new technology such as AVs. More importantly, this is a new technology whose aftercare may influence legislation on and regulation of AVs going forward.[71] Manufacturers may understandably not want the risk of unauthorized repair technicians jeopardizing the potential mass-market implementation of AVs through inconsistent repair quality.

Finally, there are legal blockades to a successful passing of right-to-repair legislation as well. For one, there is a preemption question. The DMCA "criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works and also criminalizes the act of circumventing such an access control." Copyrighted works certainly covers software, including DRM software, which is present in most of our consumer electronics devices and of course, many automobiles.[72] It is common for OEMs to sue defendants who copy software to use on replacement parts and controls, especially where the code has locks to prevent such copying.[73] Essentially, breaking this lock

67. Greenberg, *supra* note 5.

68. FDA *supra* note 53 at 1.

69. *Id.* at 23.

70. *Id.* at 17.

71. Agam Shah, *Can You Repair What You Own?*, MECHANICAL ENGINEERING, Sep. 2018 at 37.

72. It has been long established that software is an original work of fixed authorship that is copyrightable. *See, e.g.*, *Autodesk*, 621 F.3d 1102 at 1106 – 07.

73. *See, e.g.*, Andrew Thompson, *How Digital Copyright Law is Being Used to Run*

constitutes as circumvention of an access control – the exact type of action criminalized by the DMCA.

Importantly, since self-driving vehicles at higher levels of autonomy would be substantially integrated with software, repairing, and tinkering with their software would be subject to similar restrictions under the DMCA. State legislative committees are already cognizant of the complicated conflicts and questions that right-to-repair may create in relation to copyright law.[74] OEMs in the automobile industry already commonly cite the DMCA as reasons for why unauthorized repair or tinkering violates their intellectual property rights, and it is predictable that they would seek to protect their intellectual property interests for AVs as well.

Federal preemption of right-to-repair laws is also a concern when considering the DMCA. Federal preemption can be express or implied depending on the text of a given statute.[75] The former occurs where the statute's language expressly preempts state law, and the latter occurs where Congress has left no room for state regulation in the field, or where the state law conflicts with the federal regulation or is an obstacle to the federal objective.[76] Of course, there is a colorable argument to be made that the DMCA does not preempt state right-to-repair legislation, even where these repair laws would expressly allow independent repair technicians and consumers to circumvent access controls. Federal preemption of right-to-repair legislation would occur through a combination of § 301 (the "Copyright Preemption Statute") of the Copyright Act of 1976 ("Copyright Act") with the DMCA.[77]

The Copyright Preemption Statute *expressly* preempts those state laws that first, fall within the scope of copyrightable subject matter, and second, grant rights that are "equivalent to any of the exclusive rights within the general scope of copyright."[78] The argument here is that state legislatures do not

---

Roughshod Over Repairs, MSNBC (Aug. 21, 2016) https://www.nbcnews.com/news/us-news/how-digital-copyright-law-being-used-run-roughshod-over-repairs-n628606 (illustrating how OEMs such as GM have pursued action against those independent repairers seeking to circumvent software barriers to repair by copying them).

74. Daniel Moore, *You Gotta Fight For Your Right-to-Repair: The Digital Millennium Copyright Act's Effect on Right-to-Repair Legislation*, 6 TEX. A&M L. REV. 509, 517 (2019).

75. *Gade v. Nat'l Solid Wastes Mgmt. Ass'n*, 505 U.S. 88, 98 (1992) (plurality opinion).

76. *See id.*; *see also* Moore *supra* note 73 at 519.

77. 17 U.S.C. §301 (2018).

78. 17 U.S.C. § 301; Ryan v. Editions Ltd. W., 786 F.3d 754, 760 (9th Cir. 2015); accord Forest Park Pictures v. Universal Television Network, Inc., 683 F.3d 424, 429 (2d Cir. 2012); Wrench LLC v. Taco Bell Corp., 256 F.3d 446, 453 (6th Cir. 2001); *see also* Moore *supra* note 73 at 519.

intend for right-to-repair laws to be copyright laws, and that Congress itself did not intend the DMCA to be a copyright law – and as such, the Copyright Preemption Statute does not apply to the DMCA and is unable to preempt state laws.[79] In addition, such state regulation may not be expressly preempted either in those cases where the regulation has added elements.[80]

However, it is unlikely that this would be the case. Regardless of an inspection of legislative history of either the DMCA or right-to-repair laws that may be passed by state legislature, the question is not superseded by one of intent. Instead, the analysis is quite simple. Primary focus should be placed on the elements of the subject matter requirement and general scope requirement. And it is quite clear that right-to-repair laws dealing with software access controls certainly meet the first prong of this test because it is well established that software constitutes the type of expression entitled to copyright protection.[81] Moreover, such laws would not be beyond the general scope requirement because the circumvention of access controls is not "qualitatively different" from rights that the DMCA seeks to prevent – in fact, they are the exact same. Neither is it likely that the courts would view state right-to-repair legislation for AVs, which are so intertwined with software and access controls, as containing additional elements so as to make the state claim qualitatively different.[82]

PART III: THE "SOLUTION"

Introducing higher levels of autonomy into the general public requires careful attention to safety and security, and at such a crucial introductory stage in the process, manufacturers are highly incentivized against risking their investments and reputations for the sake of consumer and independent technician interests. As illustrated above, AVs offer uniquely heightened challenges to security and safety than have previous sectors that were popular with the right-to-repair coalition. Moreover, insurmountable barriers such as copyright protection from the DMCA and the need to prove the safety and security of AVs remains of paramount importance.

This is not to say that no repair-related heuristics and schematics should be made available to independent repair technicians and the general public. In fact, such a conclusion flies in the face of American traditions around

79. Moore *supra* note 73 at 519-21.

80. *Id.*

81. *See, e.g.*, Oracle Am., Inc. v. Google Inc., 750 F.3d 1339, 1355 (Fed. Cir. 2014) (finding it "well established that copyright protection can extend to both literal and non-literal elements of a computer program"); Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 702 (2d Cir. 1992).

82. Courts have traditionally taken a restrictive view of what extra elements transform an otherwise equivalent claim into one that is qualitatively different. Briarpatch Ltd., L.P v. Phoenix Pictures, Inc., 373 F.3d 296, 306 (2d Cir. 2004).

freedom of ownership and repair. Moreover, the discourse around right-to-repair brings forth important concerns that current manufacturers may find noteworthy to take heed of.

First, it is important to realize that there are systematic delays and undue expenses in dealer-monopolized repair schemes. Dealers may be unequipped to absorb the demand for small, minor fixes on a commercial scale. Since automated vehicles have not yet been widely adopted, manufacturers are able to plan ahead and start fostering more expansive networks that will be able to service their customer's needs. As such, expanding existing authorized repair technician networks and ensuring that authorized repair centers have the complete schematics, manuals, and tools they need is a crucial step that OEMs need to take. Expanded autonomy for authorized repair centers is extremely crucial on this point.

In such a scenario, the discussion on right-to-repair does not necessarily need to lead to legislation (though legislation will likely be necessary due to the above-mentioned incentives OEMs have against right to repair interests). However, manufacturers have been known to loosen up and work with consumers, especially pending legislation.[83] Such legislation may not always be the optimal way to ensure cheaper and more accessible repairs for consumers, regardless. Moreover, manufacturers have been known to offer consumer-friendly benefits in an effort to create a foundational, critical mass of consumers for groundbreaking products. For example, Tesla has intermittently offered free Supercharging programs, either unlimited or based on referrals, on its Model S and Model X vehicles in response to market demands.[84] Similarly, such creative and market-responsive efforts could be echoed for AVs as well, especially by offering comprehensive and reactive after-purchase care and services.

In addition, it would not make sense to disallow independent repair technicians from maintaining or servicing AVs in every capacity. For example, switching out faulty sensors or tires should be tasks that independent repair technicians can be given the repair capital to perform safely. Importantly, it is worth noting that just as farmers used Ukrainian firmware in order to hack into their otherwise bricked tractors, so too may frustrated consumers decide to turn to black markets or other, under the radar

83. Jake Putnam, *Right to Repair Situation Improves*, IDAHO FARM BUREAU FEDERATION (Jan. 07, 2020) https://www.idahofb.org/News-Media/2020/01/right-to-repair-situation-improves.

84. *See, e.g.*, Fred Lambert, *Tesla Removes Free Supercharging on Model S and Model X*, ELECTREK (May 27, 2020) https://electrek.co/2020/05/27/tesla-removes-free-supercharging-model-s-x/; Luke Wilkinson, *Tesla to Offer Unlimited Supercharger Access to New Customers*, AUTO EXPRESS (Aug. 05, 2019) https://www.autoexpress.co.uk/tesla/model-s/106168/tesla-to-offer-unlimited-supercharger-access-to-new-customers.

options to address their quick fix needs. As such, it is even more crucial that they have the repair manuals and heuristics that will ensure that their "quick fix" does not turn into a catastrophic accident.

As such, governments should assess the needs of the general repair community to identify those repairs that can and should be made with ease and minimal detriment to consumer security. Manuals and diagnostic tools that dealers use should be made widely available in order to ensure such safer repairs. Going further: states and the National Highway Traffic Safety Administration ("NHTSA") should require each major OEM to implement a publicly accessible repair program containing re-education or certification processes that would authorize more independent repair technicians to combat those frequent and simpler fixes without unduly jeopardizing driver safety.

Under such a scheme, manufacturers or governments should also set up a tiered security clearance system that may sufficiently protect consumer's data privacy rights as they relate to telematics and other types of data collected by AVs. This is further complicated by the fact that every jurisdiction seems to have a different idea on how to evaluate cyber security and data privacy issues. While certain privacy laws such as the European Union's General Data Protection Regulation ("GDPR") harmonize data privacy laws across a wide geographical expanse, the United States has yet to enact similarly comprehensive privacy laws on the federal level.[85] As such, any security framework regarding telematics and other data collected by AVs would have to be tailored jurisdictionally due to the "patchwork" quilt characteristic of data privacy laws in the United States and abroad.[86] Taken together, these suggestions may prove as necessary steps to take in order to facilitate the much needed mass-market penetration of AVs.

CONCLUSION

Automated vehicles will be the catalyst to jumpstart a long overdue revolution of the transportation industry as we know it. The benefits of AVs, such as increases in drivers' safety, provision of critical mobility, and fuel

85. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L. 119) 1. On the other hand, states such as California have implemented their own consumer privacy laws such as the California Consumer Privacy Act ("CCPA"), which became effective on January 1, 2020. Cal. Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100-1798.199 (Deering 2020). Such individual state efforts contribute to the patchwork characteristics of data privacy systems the world over.

86. Lorelei Laird, *Cybersecurity Laws are a Worldwide but Evolving Patchwork*, ABA JOURNAL (Mar. 18, 2016) https://www.abajournal.com/news/article/cybersecurity_laws_are_a_worldwide_but_evolving_patchwork.

savings are maximized post mass-market implementation.[87] However, one of the most insurmountable obstacles is the price barrier to entry – and as such, increasing access to maintenance and repair through right-to-repair legislation is an important avenue to consider.

Yet in the context of the nascent AV industry, right-to-repair legislation is unlikely to be successful, and may be riskier or may prove judicially improbable due to heightened challenges to security. For AVs, which necessarily include an extremely high, near unprecedented level of software integration, cybersecurity vulnerabilities can and will be accompanied by physical consequences that may prove disastrous. The barren nature of legislation and regulation on AVs will incentivize OEMs to retain monopolistic control over repair manuals and replacement parts, because any risk of inconsistent or faulty services and repair by independent repair technicians would jeopardize the entire landscape going forward. Finally, the dominance of software in AVs means that it is highly likely that the DMCA would preempt any legislation along the lines of right-to-repair for AVs, even if a state took such a brave step.

In conclusion, right-to-repair legislation will not prove successful for AVs now, or any time in the near future. Regardless, it is important that OEMs and legislature take note of the various concerns that right-to-repair supporters bring up. Chief among these concerns are that access to repair and maintenance must be made easier and more affordable. Such issues can be combated by investing more in existing repair networks, identifying those fixes that occur frequently and are relatively simple to fix, and ensuring the data privacy of drivers owning these vehicles. Maybe not just anyone should get to operate on Herbie, but we need to make sure it is easier and cheaper to find someone who can.

87. Daniel J. Fagnant & Kara Kockelman, *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations*, 77 TRANSP. RES. PART A: POL'Y & PRAC. 167, 175 (2015).