

OPEN CARS

Lothar Determann[†] & Bruce Perens^{††}

ABSTRACT

The car of the future will be autonomous, connected and full of innovative information technology features. We may drive it or let it drive us. We know it will be a computer network on wheels. However, we do not know how *open* the car of the future will be. Will it be like a desktop PC upon which we can select either Windows or Linux and choose a video card that meets our specific needs, or as closed as a DVD player with region control?

In our Article, we examine facts and arguments regarding how open the car can, should and may be, as a matter of technology, economics, public policy, and law. To make our points, we will a tale of two cars: it may be open, it may be closed. It may be the best of cars, it may be the worst of cars. We do not aim for an exact prediction regarding the degree of openness for future cars. Rather, we intend to open a public discussion and assist companies in strategic planning by highlighting the economic and policy interests as well as legal rules regarding the opening or closing of automotive designs.

Current law is not holding the open car back. Right-to-repair statutes and competition laws are providing tailwind. Intellectual property laws do not present any insurmountable obstacles to openness. Automotive product and safety rules have not (yet) dictated a path in either direction, open or closed. Onboard diagnostic ports—originally required in the interest of emission control by the California government—have become a gateway to openness and transparency.

However, product liability concerns and the phantom menace of cybersecurity could establish road blocks if manufacturers of open cars are held responsible for risks created by third party software or parts. Automakers may be reluctant to open their products further—or may even decide to lock products down—if they are indiscriminately held responsible for cyberattacks and other harm created by open cars. Sector-specific legislation and regulation may be required if courts take a wrong turn in this respect. The law must play its role to help make the open car the best of cars, and this Article takes a crucial first step in that direction by offering guidance to policymakers, judges, and manufacturers.

DOI: <https://dx.doi.org/10.15779/Z38XD0QX6F>

© 2017 Lothar Determann & Bruce Perens.

[†] Lothar Determann teaches computer, internet, and data privacy law at Freie Universität Berlin; University of California, Berkeley School of Law; and Hastings College of the Law, San Francisco. He also practices technology law as a partner with Baker & McKenzie LLP in Palo Alto, and is admitted in California and Germany.

^{††} Bruce Perens is one of the founders of the Open Source movement in software, a programmer, technologist, and intellectual property specialist, and CEO of two companies: Legal Engineering and Algoram. Opinions expressed herein reflect only the authors' views, and should not be imputed to their universities, firms, clients, or others. The authors are grateful for valuable input, research and edits by Arjun Adusumilli and Andrea Tovar.

TABLE OF CONTENTS

I.	INTRODUCTION	917
II.	CARS AND OPENNESS: NEW PATHS AND CROSSROADS	918
	A. COMPUTER ON WHEELS.....	918
	B. ECONOMIC VISIONS OF CARS AND AUTOMOTIVE BUSINESS MODELS	920
	C. DIFFERENT SPEED OF OBSOLESCENCE OF AUTOMOBILES AND COMPUTERS	923
	D. PLACE FOR THE DRIVER IN THE OPEN CAR?	925
	E. OPEN DESIGNS AND LOCKS.....	927
	F. OPEN AND PROPRIETARY BUSINESS MODELS.....	928
	1. <i>Razors, Razorblades, and Other Consumer Products</i>	928
	2. <i>Manufacturing Equipment: Ingredients and Parts</i>	929
	3. <i>Personal Computers and Software</i>	929
	4. <i>Automotive Sector</i>	931
III.	PUBLIC POLICY CONSIDERATIONS REGARDING THE OPEN CAR	934
	A. THE OPEN CAR AND ITS ENEMIES.....	934
	1. <i>Economic Interests</i>	934
	2. <i>Safety Policies</i>	935
	3. <i>Ignorance</i>	935
	B. POLICY CONSIDERATIONS FOR AND AGAINST THE OPEN CAR	937
	1. <i>Economic Freedoms</i>	937
	2. <i>Cybersecurity: The Phantom Menace</i>	939
	3. <i>Health and Safety</i>	942
	4. <i>Environmental Sustainability</i>	944
	5. <i>Consumer Protection and Prices</i>	944
	6. <i>Innovation and Intellectual Property Protection</i>	944
	7. <i>Personal Property Protection</i>	945
	8. <i>Data Privacy</i>	945
	9. <i>Summary of Policy Considerations For and Against the Open Car</i>	947
	C. POSSIBLE DEGREES OF OPENNESS FROM A TECHNICAL PERSPECTIVE	948
IV.	THE OPEN CAR AND CURRENT LAW	950
	A. MOTOR VEHICLE SAFETY LAWS.....	950
	B. EMISSIONS CONTROLS AND OPEN PORTS.....	954
	C. “RIGHT TO REPAIR” LEGISLATION AND SELF-REGULATION	959

D.	TELECOMMUNICATION LAW REQUIREMENTS ON CONNECTED CARS AND TELEMATICS SERVICES	960
E.	COMPETITION	962
	1. <i>Tying by Contract, Refusal to Deal or Design</i>	962
	2. <i>Exclusionary Practices, Monopolization</i>	966
	3. <i>Warranty Voidance</i>	967
F.	INTELLECTUAL PROPERTY LAWS	968
	1. <i>Utility Patents</i>	968
	2. <i>Design Patents</i>	971
	3. <i>Copyright Law</i>	973
	4. <i>Computer Interference Laws</i>	975
	5. <i>Trademark Law</i>	977
	6. <i>Trade Secret Law</i>	978
G.	DATA PRIVACY AND OWNERSHIP	978
	1. <i>Data Privacy Laws</i>	978
	2. <i>Data Ownership</i>	982
H.	PRODUCT LIABILITY.....	984
V.	CONCLUSIONS AND OUTLOOK: QUO VADIS, OPEN CAR?	987

I. INTRODUCTION

The car of the future will be autonomous, connected, and full of innovative information technology features. We may drive it or let it drive us. We know it will be a computer system on wheels. What we do not know is how *open* the car of the future will be. Will it be like a desktop PC upon which we can select either Windows or Linux¹ and choose a video card that meets our specific needs, or as closed as a DVD player with region control which refuses to play movies purchased overseas?²

The *open* car supports an aftermarket in which third-party manufacturers produce accessories for the vehicle, including ones not envisioned by the original manufacturer. Such accessories not only include fixtures that can be suction-cupped to the windshield like a GPS or phone, but also accessories that must integrate into the vehicle and its interfaces beyond power, the speakers, and microphone. For example, an interesting

1. Carla Schroder, *Replace the Retiring Windows XP with Linux*, LINUX FOUND. (Apr. 8, 2014), <https://www.linux.com/learn/replace-retiring-windows-xp-linux>.

2. Robert Silva, *What You Need to Know About DVD Region Codes*, LIFEWIRE (June 4, 2017), <https://www.lifewire.com/dvd-region-codes-1845720>.

potential “accessory” would be a self-driving computer or accident-preventing sensor that could be purchased separately from the vehicle and plugged into it.

In this Article, we examine facts and arguments regarding how open the car can, should, and may be as a matter of technology, economics, public policy, and law. To make our points, this Article will tell a tale of two cars: one which is open, one which is closed. It may be the best of cars, it may be the worst of cars. This Article does not aim for an exact prediction or recommendation regarding the degree of openness for future cars. Rather, the Article intends to start a public discussion and contribute to the strategic planning of companies by highlighting the economic and policy interests as well as legal rules regarding the opening or closing of automotive designs.

Part II provides an overview regarding the current state of automotive technology and concepts of openness in business models, technology, and law. Part III introduces the enemies of the open car, examines policy considerations for and against openness, and then formulates requirements regarding openness for the open car. Part IV analyzes how current law and regulatory mechanisms accelerate or provide road blocks for open and closed cars. Part V then summarizes our conclusions.

II. CARS AND OPENNESS: NEW PATHS AND CROSSROADS

Open and closed cars will race each other and compete on global markets. They have to drive on the same roads, transport the same kinds of drivers and passengers, satisfy the same expectations regarding price and functionality, comply with the same laws and safety standards, and generate profits for their makers. But they will be products of very different business models and technical architectures—one open and one closed.

A. COMPUTER ON WHEELS

The first computer was integrated in a new automobile in 1968.³ Computers that manage a vehicle’s conformance to pollution emissions standards⁴ have been required since the 1980s. Today, a typical car contains

3. *Computer Chips Inside the Car*, CHIPSETC.COM, <http://www.chipsetc.com/computer-chips-inside-the-car.html> (last visited Sept. 17, 2017).

4. *On-Board Diagnostic II (OBD II) Systems – Fact Sheet / FAQs*, CAL. AIR RES. BD. (Oct. 28, 2015), <https://www.arb.ca.gov/msprog/obdprog/obdfaq.htm>.

dozens of computers and over 100 million lines of software code.⁵ Premium automobiles increasingly assist and even override the driver with systems called “lane assist,”⁶ “summon,”⁷ “collision avoidance,”⁸ and even “autopilot.”⁹ Computerized systems that assist the driver in avoiding skids during braking are required of all new vehicles in the United States and European Union.¹⁰

Future vehicles will only become more computerized. Development will progress from driver–assistance systems to fully autonomous automobiles and trucks that take on the role of the driver. These systems will assume primary responsibility for life and property in and around the vehicle, performing as directed with or without a human present. These activities could include transporting children under the orders of their parents without any adult’s presence and conveying intoxicated individuals safely¹¹ without granting them manual control of the vehicle. As the unyielding focus of machines grows to outperform the less reliably attentive human driver, manual driving on public roads could become actionable as a safety violation.¹²

Vehicle computers have euphemistically been called “Electronic Control Units” (ECUs) since the 1980s when manufacturers expected that the customer would distrust having a computer integrated into their car.

5. Doug Newcomb, *The Next Big OS War Is In Your Dashboard*, WIRED (Dec. 3, 2012, 6:30 AM), <https://www.wired.com/2012/12/automotive-os-war/>.

6. *Lane Assist*, VOLKSWAGEN, <http://en.volkswagen.com/en/innovation-and-technology/technical-glossary/spurhalteassistentlaneassist.html> (last visited Sept. 17, 2017).

7. *Summon Your Tesla from Your Phone*, TESLA BLOG (Jan. 10, 2016), <https://www.tesla.com/blog/summon-your-tesla-your-phone>.

8. John Linkov, *Collision-Avoidance Systems Are Changing the Look of Car Safety*, CONSUMER REP. (Dec. 17, 2015), <http://www.consumerreports.org/car-safety/collision-avoidance-systems-are-changing-the-look-of-car-safety/>.

9. *Upgrading Autopilot: Seeing the World in Radar*, TESLA BLOG (Sept. 11, 2016), <https://www.tesla.com/blog/upgrading-autopilot-seeing-world-radar>.

10. *Electronic Stability Control*, SAFERCAR.GOV, <http://www.safercar.gov/Vehicle+Shoppers/Rollover/Electronic+Stability+Control> (last visited Sept. 17, 2017).

11. Lynn Walford, *How Ignition Interlock Devices Can Stop Drunk Drivers in Their Tracks*, PCWORLD (June 11, 2014, 5:30 AM), <http://www.pcworld.com/article/2362002/how-ignition-interlock-devices-can-stop-drunk-drivers-in-their-tracks.html>.

12. Jay Samit, *Driving Your Car Will Soon Be Illegal*, TECHCRUNCH (Aug. 11, 2015), <http://social.techcrunch.com/2015/08/11/driving-your-car-will-soon-be-illegal/>; Jessica S. Brodsky, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit The Brakes on Self-Driving Cars*, 31 BERKELEY TECH. L.J. 851 (2016) (exploring potential torts associated with the development of self–driving cars).

Over time, fear of computers was replaced with acceptance and finally desire, as the most attractive features of modern vehicles were implemented through computer control.¹³

The modern car has been dubbed “computer on wheels,”¹⁴ but it has become much more than one computer. Behind the operation of a modern vehicle is neither an “Electronic Control Unit” nor even a single computer, but multiprocessor networks of dozens of small computers which each control a different subsystem and communicate across the rest of the vehicle via two or more private on-board networks. At least one on-board network—often a CAN bus¹⁵ (for Controller–Area Network)—is tasked with the vital operation of the engine, traction components, and brakes and other features that affect the safety of the vehicle, while a second one—sometimes a MOST bus¹⁶ (for Media-Oriented Systems Transport)—handles driver and passenger entertainment.¹⁷

B. ECONOMIC VISIONS OF CARS AND AUTOMOTIVE BUSINESS MODELS

Consumers select the make and model of automobiles with increasing focus on information technology features: telematics, driver assistance, autonomous driving, connectivity, entertainment, and various safety

13. Doug Newcomb & Alex Colon, *The Best High-Tech Cars of 2017*, PC MAG. (Aug 10, 2017, 10:53 AM), www.pcmag.com/article2/0,2817,2477057,00.asp; David Zax, *How Car Companies Are Trying to Win Back Millennials*, CITYLAB (Sept. 2, 2014), www.citylab.com/design/2014/09/how-car-companies-are-trying-to-make-car-ownership-attractive-to-millennials/379377/.

14. David Sedgwick, *Cars Become Computers on Wheels*, AUTOMOTIVE NEWS (Apr. 21, 2014, 12:01 AM), www.autonews.com/article/20140421/OEM06/304219993/cars-become-computers-on-wheels.

15. See generally MARCO DI NATALE ET AL., UNDERSTANDING AND USING THE CONTROLLER AREA NETWORK (2012).

16. *Welcome to the MOST Cooperation*, MOST COOPERATION, <http://www.mostcooperation.com/> (last visited Sept. 17, 2017) (“MOST – Media Oriented Systems Transport – is the de-facto standard for multimedia and infotainment networking in the automotive industry.”).

17. See General Motors LLC, Comment Letter on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 6 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2017/General_Motors_class17_1201_2014.pdf; see also Jim Motavalli, *The Dozens of Computers That Make Modern Cars Go (and Stop)*, N.Y. TIMES (Feb. 4, 2010), www.nytimes.com/2010/02/05/technology/05electronics.html; Robert N. Charette, *This Car Runs on Code*, IEEE SPECTRUM (Feb. 1, 2009, 5:00 AM), <http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>.

features.¹⁸ This gets entrepreneurs thinking about new ways to earn profits in the automotive sector: companies with a background in online services may envision the car of the future as a data generator that they can give away free of charge in return for behavioral data that they can monetize for advertising and other purposes.¹⁹ Social media companies may push for a socially connected car²⁰—the next platform after the personal computer, smartphone, and virtual reality headset. Companies with strong content portfolios may view the car as a platform to distribute for video and audio material.²¹ Traditional car manufacturers may continue to focus on driving enjoyment (which Volkswagen famously marketed as “Fahrvergnügen”²²) rather than electronic distractions.²³

Different economic visions and business plans come with different preferences regarding technological openness. More likely than the extremes, future cars will more likely fall somewhere in the middle between completely open or locked-down. They will be open in some respects, closed in others. Manufacturers might compete on openness so that consumers can choose between more open and closed products.

The smartphone and its wearable progeny may have conclusively won the battle to be the customer’s ever-present electronic assistant, unless a day comes when networking is embedded in the human body.²⁴ It is not yet known whether future automobiles can profitably share the role of digital

18. THOMSON REUTERS, THE STATE OF INNOVATION IN THE AUTOMOTIVE INDUSTRY 2015 (2015), <http://ip-science.thomsonreuters.com/ip/SOI-Automotive-Industry-Report.pdf>.

19. MCKINSEY & CO., CAR DATA: PAVING THE WAY TO VALUE-CREATING MOBILITY (2016), https://www.mckinsey.de/files/mckinsey_car_data_march_2016.pdf.

20. RICHARD VIERECKL, JÖRG ASSMANN & CHRISTIAN RADÜGE, STRATEGY&, IN THE FAST LANE: THE BRIGHT FUTURE OF CONNECTED CARS (2014), http://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

21. *Nuance Launches Next-Generation Dragon Drive*, SPEECH TECH. (Nov. 13, 2013), <http://www.speechtechmag.com/Articles/News/Speech-Technology-Digest/Nuance-Launches-Next-Generation-Dragon-Drive---93249.aspx>.

22. ClassicCommercials4U, *Volkswagen Fahrvergnügen Ad from 1990*, YOUTUBE (July 13, 2009), <https://www.youtube.com/watch?v=eOnne-90CLI>.

23. Some automakers release “retro” cars with mixed results. See Ben Stewart, *6 Retro Flops, and 6 Concept Cars That Should Have Replaced Them*, POPULAR MECHANICS (June 1, 2016), www.popularmechanics.com/cars/g1287/6-retro-flops-and-6-concept-cars-that-should-have-replaced-them/.

24. See, e.g., Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. (forthcoming 2017) (describing the potential dangers with increasingly sophisticated digital assistants like Siri).

assistant with a more personal device.²⁵ Vehicles will supplement the “assistant” functions currently provided by smartphones by offering additional senses and outputs, whether the computer using them is worn or driven.

Today, smartphone applications remind you where you parked.²⁶ Some proactively prompt you and point out nearby restaurants and convenience stores.²⁷ They access your calendar and suggest routes to your next appointment.²⁸ Such applications are able to use even more specific data—such as the time of day and a history of restaurants you have parked at—in order to identify you as a likely customer and present you with a customized prospect of visiting a nearby restaurant. App manufacturers will sell this service to restaurants, and the ones that pay will likely be preferred, if not exclusively recommended.

The vehicle of the future may be equipped to sense medical data²⁹ noninvasively in order to tell if the driver is intoxicated, sleepy, or ill and to deny control of the vehicle or call for help appropriately. Infrared cameras can sense body temperature and respiration parameters³⁰ such as rate, depth, and regularity, and even the driver’s emotions.³¹ Chemical sensors can detect alcohol and perhaps other chemicals on the breath. If a vehicle carries such medical sensors, the vehicle–connected computer might also use the

25. Bill Howard, *Car Navigation Is a Ripoff. Here’s Why*, EXTREMETECH (Sept. 15, 2011, 3:31 PM), <http://www.extremetech.com/extreme/96175-car-navigation-is-a-ripoff-here’s-why>.

26. Jon Russell, *Google Now Adds Parking Reminder*, NEXT WEB (Apr. 30, 2014), <http://thenextweb.com/google/2014/05/01/google-now-gets-parking-detector-remind-left-car/>.

27. Danny Sullivan, *Google Now Adds 70 New Apps, Including Zipcar & Restaurant Bill Pay Via OpenTable*, SEARCH ENGINE LAND (Apr. 28, 2015, 2:06 PM), <http://searchengineland.com/google-now-new-apps-219906>.

28. Paul Sawers, *Waze for Android Taps Your Calendar Events to Tell You When to Leave Based on Traffic Conditions*, VENTUREBEAT (Mar. 10, 2016, 6:43 AM), <http://venturebeat.com/2016/03/10/waze-for-android-taps-your-calendar-events-to-tell-you-when-to-leave-based-on-traffic-conditions/>.

29. Press Release, Invents Co., *The Emergency Medical Assist™: A Sensor System Designed for Automobiles That Monitors the Vital Signs of the Driver* (Apr. 9, 2016), <https://invents.newswire.com/news/the-emergency-medical-assist-a-sensor-system-designed-for-automobiles-9901699>.

30. Jin Fei & Ioannis Pavlidis, *Analysis of Breathing Air Flow Patterns in Thermal Imaging*, PROC. 28TH IEEE EMBS ANN. INT’L CONF. 946–52 (2006).

31. Elisa Campo, *Thermal Imaging Cameras to Read Human Emotions*, IEN EUR. (Nov. 5, 2015), <https://www.ien.eu/article/thermal-imaging-cameras-to-read-human-emotions/>.

data from them to assess whether the driver and passengers are hungry and monetize that as an advertising opportunity. It might assess sleepiness and point out a motel, asking if it should make a reservation, and completing the booking if approved.³² It will certainly be aware of the amount of remaining fuel and will point out gas or recharge stations as appropriate.³³

C. DIFFERENT SPEED OF OBSOLESCENCE OF AUTOMOBILES AND COMPUTERS

Consider the time until obsolescence of a smartphone³⁴ versus that of a modern automobile. A 1950s car, maintained appropriately, can still operate safely and even be fun to drive. In contrast, the owner of that automobile is not likely to keep a smartphone for longer than four years. Moore's law³⁵ still applies to computers, which means that the CPU speed and memory capacity of new smartphones doubles close to annually. Thus, while phones in 2006 did not have good cameras and barely had practical web browsers, today's phones integrate excellent cameras, can easily present not only web pages but feature films, and (with server support over the internet) can understand your voice and reply appropriately.³⁶

Integrated navigation systems in automobiles have been a technical and economic failure, in that they are generally supplanted by a more capable program in a smartphone within a few years of a new automobile's sale, and the user generally abandons use of the onboard system.³⁷ Integrated entertainment systems that offer network services and apps suffer from similar problems: they are supplanted by more powerful apps on an up-to-date smartphone. From then on, the user employs the on-board entertainment system mainly for the Bluetooth path that connects a

32. Eric Ravenscraft, *Google Now Adds Gas Stations On Your Route Cards*, LIFEHACKER (Feb. 23, 2015, 7:30 AM), <http://lifehacker.com/google-now-adds-gas-stations-on-your-route-cards-1687419012>.

33. *Id.*

34. Chris Ely, *The Life Expectancy of Electronics*, CONSUMER TECH. ASS'N (Sept. 16, 2014), <https://www.cta.tech/News/Blog/Articles/2014/September/The-Life-Expectancy-of-Electronics.aspx>.

35. Chris Mack, *The Multiple Lives of Moore's Law*, IEEE SPECTRUM (Mar. 30, 2015, 3:00 PM), <http://spectrum.ieee.org/semiconductors/processors/the-multiple-lives-of-moores-law>.

36. Casey Phillips, *How Smartphones Revolutionized Society in Less Than a Decade*, GOV'T TECH. (Nov. 20, 2014), <http://www.govtech.com/products/How-Smartphones-Revolutionized-Society-in-Less-than-a-Decade.html>.

37. Howard, *supra* note 25.

smartphone to an automobile's speakers and provides a speakerphone microphone for telephone calls.³⁸

For a time, there can be software updates to the on-board computers of vehicles. However, auto manufacturers charge prices approaching that of a new smartphone for only a few year's updates, and manufacturers (with the notable exception of Tesla³⁹) have historically not added many new software features to their years-old automobile models, preferring to use the desire for features to drive the sale of new automobiles.⁴⁰

Within a few years, the computer hardware behind a navigation or entertainment system is typically eclipsed by the capability of newer models and further software updates must be limited to the capabilities of the old system. Auto manufacturers have not, so far, offered new electronics to upgrade old cars. This, again, is considered an opportunity for a new vehicle sale.⁴¹

But this paradigm of old vehicles continuing to contain old computers for their entire useful lives will not be sufficient to support the advent of autonomous vehicles. The technology of autonomous vehicles will go through very rapid development throughout the next several decades. For at least the next decade, a system only three years old can be expected to significantly trail the capabilities of newer systems, to an extent great enough that its capability for safe operation can be considered unacceptable when compared to a new system. Thus, it is likely that manufacturers will integrate planned obsolescence into these systems so that the autonomous feature is deactivated some years after purchase unless the system hardware has been updated, and the autonomous feature will be deactivated within months if the owner somehow misses software updates. This places an end-date on the occurrence of events that would lead to liability of the manufacturer for a particular software and hardware version.⁴² Rather than

38. David Pogue, *Why the Upgrade Cycle Will Never End*, SCI. AM. (June 1, 2015), <https://www.scientificamerican.com/article/why-the-upgrade-cycle-will-never-end/>.

39. Fred Lambert, *Tesla Roadster 3.0 Battery Upgrade (R80) Are Finally Starting to Arrive—340 Miles of Range*, ELECTREK (July 8, 2016, 5:43 AM), <https://electrek.co/2016/07/08/tesla-roadster-3-0-battery-upgrade-r80/>.

40. Pogue, *supra* note 38.

41. *Id.*

42. Tesla is able to continue to improve its computer-rich model *S* and *X* automobiles because their owners have paid around \$100,000 per car and are willing to put in \$20,000 per upgrade. See Fred Lambert, *Tesla Now Offers Almost \$20,000 in Software-Upgradable Options When Buying a Vehicle*, ELECTREK (Oct. 26, 2016, 8:23 AM), <https://electrek.co/2016/10/26/tesla-now-offers-almost-20000-in-software-upgradable->

sell autonomous vehicles, manufacturers could lease them, with the lease payment including periodic system upgrades to keep the autonomous function up to the state of the art, or just offer cars on a subscription basis with a limited time use of hardware included in the service, adding Car-as-a-Service (CaaS) offerings to SaaS, PaaS, IaaS,⁴³ and other phenomena in the cloud economy.

D. PLACE FOR THE DRIVER IN THE OPEN CAR?

Pilots have to be checked out in airplane makes and models before they can fly a new plane solo.⁴⁴ Pilot training and license requirements for manned and unmanned aircraft and flying in visual and instrument flight conditions vary greatly. With respect to automobiles, driver license schemes differentiate between permissions to drive trucks, motorcycles, and cars, but not (yet) within the category “passenger car.” This may have to be reconsidered as cars get more complicated, drivers may become less involved in the details of operating a car and different models may function very differently, because the driver of an older automobile with manual gear shifting requires a different skillset than the operator of an autonomous car.

Another question to consider is whether the autonomous driving function of an automobile must be one manufactured only by the manufacturer of that vehicle and nobody else. Traditional auto manufacturers, daunted by their corporate inexperience with autonomous vehicles and fear of tremendous liability as they take on the role of driver for the first time, may argue that only they know how to integrate such a function safely into their own vehicles. However, it is technically possible to create a standard interface for autonomous driving systems, providing a standard set of sensors and vehicle controls, a standard space for the computer, and standard connectors to interface to it. The sensors integrated into the vehicle can themselves be replaced with newer models that include

options-when-buying-a-vehicle/. Tesla has offered a \$29,000 battery upgrade for their *Roadster* models even though there are only about 2,000 in existence. This strategy assures Tesla purchasers that their vehicle will be protected from obsolescence for a longer period than vehicles of more conventional automakers. But can Tesla sustain this practice for the affordable, mass-market model 3? It is not yet clear whether a manufacturer of more economical vehicles could continue to upgrade computers and software at the price points the owners of such vehicles could pay.

43. See Eamonn Colman, *When to Use SaaS, PaaS, and IaaS*, COMPUTENEXT (Aug. 27, 2013), <https://www.computenext.com/blog/when-to-use-saas-paas-and-iaas/>.

44. *Private Pilot Requirements*, FIRSTFLIGHT, <http://www.airbus.com/support/training/flight/flight-training-with-a350-xwb/> (last visited Sept. 17, 2017).

new features, but at longer intervals than the autonomous driving computer and while continuing to use the same wires and connectors to interface to the autonomous driving computer. Programmer George Hotz has already adapted his own creation of a self-driving computer to the existing interfaces of some modern cars, and was able to capitalize *comma.ai*, a new startup, for \$3.1 million on the strength of that demonstration.⁴⁵

Such interoperability would support more competition in the production of autonomous driving systems, potentially reducing their prices and increasing their capability. It is likely that the producers of these systems can be held to the same safety and testing standards as the automobile manufacturer. But this would require that manufacturers be willing to implement a standard, rather than exclusively own the autonomous system for their vehicles. Manufacturers might not be willing to take that step without government encouragement.

Such systems would have expiration dates for both the software and hardware, so that the system would disable the autonomous function once it is past a mandatory replacement date. This would prevent the use of “junkier” computers to drive autonomously past the date when they could be expected to perform with a level of safety comparable to more modern units, just as corporations have to remove computers with Windows 7 due to its known security issues and upgrade to a new version.⁴⁶

The addition of a capability⁴⁷ for the autonomous driving computer to be replaced using standards that allow for multiple manufacturers potentially addresses the economic problem of continuous upgrades. An owner would have a competitive market in which to purchase autonomous driving systems, and thus lower prices. Old or obsolete autonomous driving computers could be removed from a vehicle, leaving it fully functional to

45. Danny Yadron, *This 26-Year-Old Hacker Can Make A Self-Driving Car, But Can He Take On Tesla?*, GUARDIAN (Apr. 5, 2016), <https://www.theguardian.com/technology/2016/apr/05/george-hotz-comma-self-driving-car-tesla-elon-musk>.

46. Liam Tung, *Microsoft: Windows 7 In 2017 Is So Outdated That Patches Can't Keep It Secure*, ZDNET (Jan. 17, 2017, 2:34 PM), <http://www.zdnet.com/article/microsoft-windows-7-in-2017-is-so-outdated-that-patches-cant-keep-it-secure/>.

47. Rob Freeborn, *How Much Does It Cost to Replace a Vehicle Computer*, ISEECARS, <https://blog.iseecars.com/how-much-does-it-cost-to-replace-a-vehicle-computer/> (last visited Sept. 17, 2017); see also Cassandra E. Havens, *Saving Patent Law from Competition Policy and Economic Theories: Kimble v. Marvel Entertainment LLC*, 31 BERKELEY TECH. L.J. 371, 376 (2016) (describing generally how “antitrust laws protect market competition”).

be human-driven. A new owner of a used car could choose to add an autonomous function or not.

E. OPEN DESIGNS AND LOCKS

The first exclusion mechanism in an automobile was the door lock, an advertised feature since 1915, although it did not become universal until the 1960s. Door and starter/ignition locks operate in the interest of the vehicle owner, protecting the owner's property. More recently, exclusion mechanisms which operate in the interest of the manufacturer and contrary to the interest of the owner⁴⁸ have been added to modern vehicles, creating and protecting monopolies for the manufacturer. Such restrictions prevent the addition of some options and accessories by anyone other than a manufacturer-authorized dealer. For example, one modern American SUV model allows the physical installation of an upgraded entertainment system, but it will not function and interoperate with the rest of the vehicle's systems until authorized using a device available only to the dealer.⁴⁹

Manufacturers have many options to design their products in an open way, or in one that mandates that parts and accessories be exclusively made or authorized by the manufacturer. For example, manufacturers can adopt and help to set standards for communication protocols and physical connectors that allow car owners to swap out original radios, navigation systems, and other features for preferred aftermarket parts.⁵⁰ Or, to preferentially support sales of their own products and those of their exclusively-licensed vendors, manufacturers can prevent retrofitting, tuning, and other modifications by encrypting their internal communications, using proprietary communication protocols, and implementing nonstandard physical connectors.⁵¹ To this end, manufacturers can withhold documentation and manuals from the end-user

48. Pete Bigelow, *Automakers to Gearheads: Stop Repairing Cars*, AUTOBLOG (Apr. 20, 2015, 10:31 AM), <http://www.autoblog.com/2015/04/20/automakers-gearheads-car-repairs/>.

49. jim_87, Comment to *Uconnect 5.0 Upgrade to 8.4AN (2014 Cherokee) - Part Deux*, JEEP CHEROKEE FS. (Apr. 18, 2015, 5:59 PM), <http://jeepcherokeclub.com/385-jeepcherokeclub-com-how-s/123826-uconnect-5-0-upgrade-8-4an-2014-cherokee-part-deux.html>.

50. Jason Torchinsky, *Carmakers Want to Use Copyright Law to Make Working on Your Car Illegal*, JALOPNIK (Apr. 21, 2015, 12:05 PM), <http://jalopnik.com/carmakers-want-to-make-working-on-your-car-illegal-beca-1699132210>

51. Niels Koch, *The Car Entertainment System*, in NEW TRENDS AND DEVELOPMENTS IN AUTOMOTIVE SYSTEM ENGINEERING (Marcello Chiaberge ed., 2011).

and makers of aftermarket modifications, so that interoperation with their on-board electronics is impossible without extensive reverse-engineering.

F. OPEN AND PROPRIETARY BUSINESS MODELS

Most of us associate the attribute “open” with positive connotations. In open societies, individuals are free to decide, governments are transparent, accountable to individuals and tolerant.⁵² The federal government and others promote open governance.⁵³ In the information technology industry, programmers fervently promote open source code licensing.⁵⁴ Calls for open borders, open markets, open standards, open platforms, open data, and open robotics have become louder.⁵⁵ Open stands for accessible, transparent, and free from restraints. Proprietary stands for secrecy, with the information necessary to interface to a device made opaque and withheld from the user and third-party vendors, and protected with trade secret law and technical protection measures fortified by the Digital Millennium Copyright Act (“DMCA”).⁵⁶

1. Razors, Razorblades, and Other Consumer Products

Manufacturers of products that require consumable supplies often sell the main product as a “loss leader,” sometimes at a lower price than the cost of production and distribution, and the consumable at a markup that more than recovers the cost of the main product. This is called the razors-and-blades paradigm after the classic product sold using it.⁵⁷ The razors-and-blades paradigm is used, for example, in selling consumer and small-

52. KARL POPPER, *THE OPEN SOCIETY AND ITS ENEMIES* (1945).

53. White House Memorandum for the Heads of Exec. Depts. & Agencies (Jan. 21, 2009), <https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government> (identifying the Obama administration’s commitment “to creating an unprecedented level of openness in Government”).

54. Lothar Determann, *Dangerous Liaisons—Software Combinations as Derivative Works? Distribution, Installation and Execution of Linked Programs under Copyright Law, Commercial Licenses and the GPL*, 21 BERKELEY TECH. L.J. 1421 (2006); Christian Chessman, *A “Source” of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 223 (2017) (calling for the development of government funded open-source programs in criminal trials).

55. M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 577 (2011); JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET—AND HOW TO STOP IT* 3–5 (2008); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1976 (2006); 4 MELVILLE B. NIMMER & DAVID NIMMER, *NIMMER ON COPYRIGHT* § 13.03[F][5] (2013).

56. 17 U.S.C. § 1201 (2012).

57. See generally Randal C. Picker, *The Razors-and-Blades Myth(s)*, 78 U. CHI. L. REV. 225 (2011).

business printers, with low costs for the printer while the ink in cartridges for the same printer sells for a higher price by weight than gold.⁵⁸ Companies that pursue such business models cannot afford to open interfaces or connectors, as this would allow price competition upon the supplies. They rely on locks, proprietary designs, intellectual property rights, and other barriers to prevent third parties from selling consumables, parts or compatible products. Makers of video game consoles have fought prolonged legal battles to keep control over games that can be played on their consoles⁵⁹ or platforms to which their operating systems and games can be ported.⁶⁰

The razors-and-blades paradigm remains relevant in the digital era because manufacturers do not stop earning revenue when they sell their hardware. For example, they can keep a lock on online stores that purchasers of smartphones must use to add applications.⁶¹

2. *Manufacturing Equipment: Ingredients and Parts*

Somewhat similar to the razors-and-blades models in the consumer space, makers of manufacturing equipment have been trying to lock down aftermarkets for ingredients or parts. The United Shoe Machine Corporation tried to require buyers of its machines to also purchase its leather.⁶² The International Salt Company tried to require buyers of its machines to purchase its salt.⁶³ Kodak and Xerox have been trying to prohibit, prevent or discourage unaffiliated companies to supply parts, add-on products, or repair and maintenance services.⁶⁴

3. *Personal Computers and Software*

As in other markets, some computer manufacturers have also tried to keep their product environments closed. In the 1930s, for example, IBM

58. See *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004).

59. See *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

60. See *Sony Comput. Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000).

61. Larry Dignan, *Apple's App Store Revenue Tops \$28 Billion Mark, Developers Net \$20 Billion*, ZDNET: BETWEEN THE LINES, (Jan. 5, 2017, 12:08 PM) <http://www.zdnet.com/article/apples-app-store-2016-revenue-tops-28-billion-mark-developers-net-20-billion/>.

62. See *United Shoe Mach. Corp. v. United States*, 258 U.S. 451 (1922).

63. See *Int'l Salt Co. V. United States*, 332 U.S. 392 (1947).

64. Joseph P. Bauer, *Antitrust Implications of Aftermarkets*, 52 ANTITRUST BULL. 31, 34 (2007).

tried to require buyers of its punch card sorting machines to buy the actual cards also from IBM, but was challenged on similar antitrust grounds as companies with other tying models.⁶⁵

But, more than in other industries, companies in the information technology sector have also used openness to their competitive advantage and benefited from network effects. In the 1980s, Apple and Microsoft competed in the relatively new market for personal computing products. Apple implemented exclusivity on the hardware and operating system combination on Macintosh computers: you could neither install MacOS on another manufacturer's hardware nor could you run Windows upon Macintosh hardware. Microsoft, in contrast, developed an operating system that was often purchased separately from the hardware and was capable of being installed on commodity PCs from many different manufacturers. Microsoft prevailed in the personal computing market.⁶⁶

Microsoft's Office file formats were not documented to other manufacturers so that an exhaustive reverse-engineering process was responsible for competing programs to make use of the files. When Microsoft tried to extend its market power in the personal computer operating system and office application software sector to new application fields, the U.S. government intervened on antitrust grounds. It challenged Microsoft regarding its attempt to acquire Intuit Inc. and to bundle its Internet Explorer browser application with the Windows operating system.⁶⁷

More recently, Apple created an "app store" for iOS phones and tablets with tremendous economic success. The app store involves a relatively open model that other providers including Microsoft, Blackberry, and Google are trying to emulate with more or less success.⁶⁸ Consumers find a computer or software product that is interoperable and has an open market for apps and accessories more valuable than a locked-down product. With interoperable computers or smartphones, consumers can connect to specialist software applications, content (including on web and mobile sites), printers, and sensors (such as heart rate monitors or step counters).

65. IBM Corp. v. United States, 298 U.S. 131 (1936); *see also infra* note 70.

66. Matt Kapko, *History of Apple and Microsoft: 4 Decades of Peaks and Valleys*, CIO (Oct. 7, 2015, 5:00 AM), www.cio.com/article/2989667/consumer-technology/history-of-apple-and-microsoft-4-decades-of-peaks-and-valleys.html.

67. U.S. v. Microsoft: *Timeline*, WIRED (Nov. 04, 2002, 12:00 PM), www.wired.com/2002/11/u-s-v-microsoft-timeline/.

68. Google v. Apple: *Which Will Be Better in 11 Years*, CNBC (Aug. 19, 2015), <http://www.cnbc.com/2015/08/19/google-vs-apple-which-will-be-better-in-11-years.html>.

Manufacturers of information technology products cannot typically succeed if they completely lock down their products. Yet, the manufacturers are also driven to exercise a degree of control in order to extract license fees, royalties or other consideration for access to their platforms.

4. *Automotive Sector*

In the automotive sector, the battle over openness and locks on the “aftermarket,”—the sale of accessories after the original purchase of an automobile—has been focused on hardware parts for close to a century.⁶⁹ Courts have required manufacturers allow some degree of openness regarding aftermarkets while also giving them some leeway under the rule of reason, applying similar rules of the road to other cases of consumer products and manufacturing equipment.⁷⁰ But as automobiles become more computerized, their manufacturers are finding the rules of information technology markets increasingly relevant.

Manufacturers are implementing software locks to prevent the operation of aftermarket accessories without the automobile manufacturer’s authorization. But they feel market pressures towards openness as well because consumers select their car on the basis of whether it allows a seamless connection to their favorite smartphones, and fleet managers may consider whether a car connects to their preferred telematics system when they look to add to or replace their fleet. Therefore, car manufacturers suddenly find themselves in a similar situation to information technology providers: connectivity, interoperability, and openness are no longer just a threat to revenue opportunities on aftermarkets but a differentiator and essential success factor on primary and aftermarkets. Most leading car

69. See Morris A. Cohen, Narendra Agrawal & Vipul Agrawal, *Winning in the Aftermarket*, HARV. BUS. REV. (May 2006), <https://hbr.org/2006/05/winning-in-the-aftermarket>.

70. Bauer, *supra* note 64; see also, e.g., *Pick Mfg. Co. v. Gen. Motors Corp.*, 80 F.2d 641 (7th Cir. 1935), *aff’d*, 299 U.S. 3 (1936) (per curiam); *Crappon, Inc. v. Subaru of N. Am., Inc.*, 858 F.2d 792 (1st Cir. 1988); *Mozart Co. v. Mercedes-Benz of N. Am.*, 833 F.2d 1342 (9th Cir. 1987); *Metrix Warehouse, Inc. v. Daimler-Benz AG*, 828 F.2d 1033 (4th Cir. 1987); *Sherman v. British Leyland Motors, Ltd.*, 601 F.2d 429 (9th Cir. 1979); *Heattransfer Corp. v. Volkswagenwerk, A.G.*, 553 F.2d 964 (5th Cir. 1977); see also *Bob Maxfield, Inc. v. Am. Motors Corp.*, 637 F.2d 1033 (5th Cir. 1981); *Dealer Comput. Servs., Inc. v. Ford Motor Co.*, No. Civ.A. H-06-175, 2006 WL 801033 (S.D. Tex. Mar. 28, 2006).

manufacturers are already trying to create developer ecosystems similar to mobile app platforms.⁷¹

When we look at the car as a “multicomputer on wheels,”⁷² we must not forget what has traditionally been its primary functionality: transportation. Computers without wheels do not invoke the same safety and environmental concerns as cars. Car emissions threaten global climate. Car safety deficiencies threaten life and limb of drivers, passengers, cyclists and bystanders. But we should also not take for granted that cars must be more locked down than computers without wheels due to environmental and safety concerns. In fact, environmental and safety concerns also present strong arguments for openness, or at least disclosure.⁷³

A manufacturer can disclose all of the source code of its software—with all patent and copyrights reserved—to allow third parties to audit proprietary software for safety issues. Disclosure scares non-computer-professionals because they believe that it can lead to the discovery of security flaws by those who would exploit them criminally. However, properly-written software remains secure even if a criminal knows every

71. TIBCO, THE CONNECTED CAR FINDING THE INTERSECTION OF OPPORTUNITY AND CONSUMER DEMAND (2016), https://www.mashery.com/sites/default/files/fields/field_file_pdf/whitepapers/wp-mashery-the-connected-car.pdf.

72. David Sedgwick, *Cars Become Computers on Wheels*, AUTOMOTIVE NEWS (Apr. 21, 2014, 12:01 AM), www.autonews.com/article/20140421/OEM06/304219993/cars-become-computers-on-wheels.

73. For example, the Volkswagen diesel emissions scandal was only found due to scientific research which involved one of the automobiles. *See infra* Section III.B.; Jack Ewing, *Researchers Who Exposed VW Gain Little From Success*, N.Y. TIMES (July 24, 2016), <https://www.nytimes.com/2016/07/25/business/vw-wvu-diesel-volkswagen-west-virginia.html>.

detail of its operation.⁷⁴ Security researchers⁷⁵ can identify safety and security concerns more easily when the software of open cars is disclosed. They can flag security vulnerabilities and cheating regarding emission tests. Easy access for security researchers more than balances out the capability of computer criminals to glean more information from disclosed software. Computer scientists have thus in general only accepted cryptography and other security-critical software that are fully disclosed, because it is too easy to hide back-doors in opaque software. Computer scientists insist that the mathematical algorithms in cryptography software must be fully documented and must survive intensive public examination without the discovery of flaws. Open source software, which is obviously disclosed, has been found in practice to be at least as secure as locked-down software—if not more secure.⁷⁶

74. Karen Scarfone, Wayne Jansen & Miles Tracy, *Guide to Server Security*, NAT'L INST. STANDARDS & TECH. (July 2008), <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf> (“System security should not depend on the secrecy of the implementation or its components.”). The concept of security through obscurity goes back to locksmith Alfred Charles Hobbs, who in 1851 demonstrated the vulnerabilities of locks to the public, claiming that thieves had already learned them. Roman Mars, *In 1851, A Man Picked Two Unpickable Locks and Changed Security Forever*, GIZMODO (Apr. 17, 2015, 7:40 PM), <http://gizmodo.com/in-1851-a-man-picked-two-unpickable-locks-and-changed-1698557792>. It was formalized in Kerckhoff's Doctrine of 1883, which stated that a cryptosystem should remain secure even if the enemy knows everything about the system except for the cryptographic key. Xin Jan et al., *ASAP: Eliminating Algorithm-Based Disclosure in Privacy-Preserving Data Publishing*, 36 INFO. SYS. 859, 860 (2011). It was later restated by scientist Claude Shannon that systems should be designed with the assumption that the enemy will immediately acquire full knowledge of them. Anthony Langworth, *A Ticket to Security Via Obscurity*, RANDOM ACTS OF ARCHITECTURE (Nov. 14, 2012), <https://randomactsofarchitecture.com/2012/11/14/a-ticket-to-security-via-obscurity/>.

75. Terms that refer to people and groups should be used with sensitivity. In this paper we use the phrase “computer criminal” and we avoid the term “hacker”. The original meaning of “hacker” was an unconventional and astonishingly effective programmer, and many people in the computer world still refer to the best of their peers as “hackers” and resent the misapplication of the phrase to mean “criminal”. People who research computer security without criminal intent are referred to as “security researchers”, even if they do not hew to the preferences of a manufacturer regarding disclosure of their product's vulnerabilities and publicly disclose the vulnerabilities for the protection of the consumer. We do not find a need to designate either party as “white hats” or “black hats”, since their affiliation is obvious and the wearing of colored hats is significant in many religions.

76. Tom Espiner, *Trend Micro: Open Source Is More Secure*, ZDNET (June 13, 2006, 11:44 PM), www.zdnet.com/news/trend-micro-opensource-is-more-secure/148445; see also Chessman, *supra* note 54, at 223 (“Because of its transparency, open-source software empirically and categorically has fewer errors and security concerns than similarly situated

This brings us back to our tale of two cars: owners of open cars can replace or add aftermarket parts, upgrade the navigation system, or replace the entire GPS receiver. They may be able to hold on to a beautiful antique car with a fine proven motor, while keeping its technology up to date. But an open platform may also facilitate the production of poor aftermarket components that lead to accidents and injury, if those components are not carefully regulated, tested, and held to high standards. Thus, the open car may be the best of cars, it may be the worst of cars. Whichever it is, the open car will offer choices to owners, oversight by researchers, and opportunities and competition for companies after the original vehicle purchase.

Owners of a closed car will fully depend on its manufacturer for upgrades, updates and add-ons. If the manufacturer is unwilling or unable to keep systems up to date and a closed car's software becomes unsafe or unusable, the car might remain operable for manual driving only or it could become unsafe even for that. Car owners may have to decommission an otherwise perfectly good car, just as a smartphone owner might be forced to discard an otherwise-wonderful phone when the cellular network changes. Closed cars which are not updated will be ripe for exploitation by computer criminals who reverse-engineer their vulnerabilities and cause the car to be unusable or even to injure someone. The closed car may be the best of cars, it may be the worst of cars. Whichever it is, the closed car will allow the original manufacturer to retain more choices after the original vehicle sale.

III. PUBLIC POLICY CONSIDERATIONS REGARDING THE OPEN CAR

A. THE OPEN CAR AND ITS ENEMIES

Like many other revolutions, the open car will have enemies, including enemies by economic interest, enemies by public policy conviction and enemies by ignorance.

1. *Economic Interests*

Car manufacturers are interested in preventing sales of aftermarket parts and add-on products for a number of reasons, not the least of which is the

programs that are privately developed.”). *But see* Noah Gamer, *The Problem With Open Source Malware*, TREND MICRO (Feb. 23, 2016), <http://blog.trendmicro.com/the-problem-with-open-source-malware/>.

opportunity to capture the associated revenue. If car manufacturers can count on sales of aftermarket parts and products, they can make more units and benefit from economies of scale; for example, they can sell the original car at a lower price if they can count on guaranteed or highly likely sales from aftermarket parts and products. Car manufacturers also want to protect the reputation of their products, which can be harmed by low quality replacement parts or add-on products. Moreover, car manufacturers are exposed to product liability and warranty cases that can arise from situations in which it can be unclear—and costly to litigate—whether a defect or accident was caused by the original car or a third-party replacement or add-on product.⁷⁷ Manufacturers have been held responsible for defects caused by aftermarket products sold by third parties on the grounds that the original manufacturer should have warned about risks caused by add-ons.⁷⁸

2. *Safety Policies*

Law and policy makers lean towards addressing perceived risks to health and safety with laws and regulations that prohibit, prevent, or discourage openness and independence. Just as car owners lock their cars for fear of auto theft and break-ins, regulators may order interfaces to be locked up for fear of cyberattacks, unsafe aftermarket parts, and risky tinkering by hobbyists. Also, openness may suffer collateral damage from any overly detailed regulation that may not even be intended to lock up interfaces, but could result in restrictions as a side effect. For example, if law and policy makers hold car manufacturers responsible for cybersecurity risks created by aftermarket products or parts made by unaffiliated third parties, car manufacturers will be motivated to shut down access to parts in order to mitigate risk and liability.

3. *Ignorance*

Consumers often act with information deficits. When in doubt, consumers may prefer a branded product made or recommended by the original car manufacturer over a product made by third parties regardless of

77. DEREK H. SWANSON & LIN WEI, UNITED STATES AUTOMOTIVE PRODUCTS LIABILITY LAW (2009), <https://www.mcguirewoods.com/news-resources/publications/us-automotive-products-liability.pdf>.

78. *See*, BGH, 09.12.1986 VI ZR 65/86 (Honda), www.jurion.de/urteile/bgh/1986-12-09/vi-zr-65_86/; *Liriano v. Hobart Corp.*, 92 N.Y.2d 232, 242–43 (N.Y. 1998) (considering the possibility of manufacturer liability due to a failure to warn even when there is substantial post-sale modification).

quality and price considerations. Thus, original equipment manufacturers can benefit from fear, uncertainty and doubt regarding aftermarket products. To the extent that manufacturers control the retail sales narrative, they can nourish information deficits to their advantage. Car manufacturers tend to control their dealer networks quite tightly and have also been known to influence consumer tests.⁷⁹

Legislatures and regulators may also oppose openness due to information deficits. While the Environmental Protection Agency (EPA) affirmatively opposed copyright exceptions for security research and interoperability,⁸⁰ the agency was alerted by a security researcher about problematic software in Volkswagen diesel cars that manipulated emission tests.⁸¹ The independent researcher triggered a wave of investigations, media reports and regulatory action, also concerning other automakers and individual auto-suppliers.⁸² Had regulators adequately appreciated the benefits of independent research into automakers' software, they should

79. See *ADAC Admits Making Up Car Award Votes*, LOCAL (Jan. 20, 2014, 9:42 AM), <http://www.thelocal.de/20140120/adac-boss-cooks-car-award-votes>.

80. In a letter dated July 17, 2015, an Assistant General Counsel of the Environmental Protection Agency (EPA) wrote to the Copyright Office with respect to proposed Section 1201 rulemaking and argued against exceptions that the Electronic Frontier Foundation (EFF) had proposed to enable the very kind of security research that ultimately revealed the car manufacturer manipulations that the EPA then pursued with aggressive enforcement and penalties. See Letter from Geoff Cooper, Assistant General Counsel, Evtl. Prot. Agency, to Jacqueline C. Charlesworth, Gen. Counsel & Assoc. Register of Copyrights (July 17, 2015), https://copyright.gov/1201/2015/USCO-letters/EPA_Letter_to_USCO_re_1201.pdf.

81. Rupert Neate, *Meet John German: The Man Who Helped Expose Volkswagen's Emissions Scandal*, GUARDIAN (Sept. 26, 2016, 7:00 AM), www.theguardian.com/business/2015/sep/26/volkswagen-scandal-emissions-tests-john-german-research; Russell Hotten, *Volkswagen: The Scandal Explained*, BBC NEWS (Dec. 10, 2015), www.bbc.com/news/business-34324772.

82. See Patrick Welter et al., *Die Autoindustrie Unter Generalverdacht* [*Car Industry Under General Suspicion*], FRANKFURTER ALLGEMEINE (Apr. 20, 2016), www.faz.net/aktuell/wirtschaft/manipulationen-nicht-nur-bei-vw-sondern-auch-bei-mitsubishi-die-autoindustrie-unter-generalverdacht-14189868.html; *Peugeot Raided by French Emissions Investigators*, BBC NEWS (Apr. 21, 2016), www.bbc.com/news/business-36106783; Karishma Vaswani, *When Saying Sorry Is the Only Thing to Do*, BBC NEWS (Apr. 20, 2016), www.bbc.com/news/business-36093703 (referring to the Mitsubishi scandal); *Japan Officials Raid Suzuki Headquarters*, BBC NEWS (June 3, 2016), www.bbc.com/news/business-36441906; *Fiat Shares Drop on Report of Sales Ban*, BBC NEWS (May 23, 2016), www.bbc.com/news/business-36357174; AFP, *Bosch 'Helped Conceal' Volkswagen's Emissions Cheating Devices*, DAILY MAIL (Sept. 7, 2016, 8:58 PM), <http://www.dailymail.co.uk/wires/afp/article-3777880/Bosch-helped-conceal-Volkswagens-emissions-cheating-devices.html>.

have supported increased openness and not lobbied against limited exceptions for copyright restrictions on automotive software.

Finally, companies themselves may miss opportunities of open platforms due to incorrect assessments of their situation and what the market desires. Owners of intellectual property have been trained to hold it close, and may do so even when openness might lead to much greater income. For example, Research in Motion, the maker of Blackberry, was the first company to introduce handheld email receivers and seemed for a while to be the untouchable leader of smartphones for the enterprise. Nokia also held a great portion of the mobile device market. Both companies underestimated the potential of the App Store introduced by Apple, which pushed the boundaries of openness in the mobile market.⁸³

B. POLICY CONSIDERATIONS FOR AND AGAINST THE OPEN CAR

Friends and enemies can advance numerous arguments for and against the open car.

1. *Economic Freedoms*

As a starting point in a free society and economy, manufacturers should generally be able to design their products in their own discretion. So long as cars are safe and environmentally sustainable, governments should not try to micromanage the product development, design and manufacturing process. Manufacturers, dealers, consumers and other market forces can decide how open or closed cars should be. Open cars should ideally compete with closed cars on free markets to determine which model comes out ahead.

But, on a policy level, one has to take into account that all cars have to share the road and various coordination issues must be resolved through at least some standardization. In most economies, the markets of automotive products are indeed subject to heavy government intervention. Most governments view cars as a major factor for the economy, labor markets, mobility, scientific progress, safety and the environment. Governments feel a high degree of responsibility for the car sector and feel cars must operate in the public interest. In a hypothetically level and competitive market, we could let the market decide upon the degree of openness necessary, and

83. Daniel Eran Dilger, *How Apple's iPhone Destroyed Nokia's World Leading Symbian Platform*, APPLEINSIDER (Oct. 10, 2013, 12:54 AM), <http://appleinsider.com/articles/13/10/10/how-apples-iphone-rapidly-destroyed-nokias-world-leading-symbian-platform>.

allow automobile manufacturers to engineer their vehicles without government interference. But, in practice, the automotive markets are far less free than other sectors. The sheer cost of manufacturing modern automobiles that perform adequately and comply with all relevant safety and environmental rules means that only a few companies, funded with many billions of dollars, can afford to participate in automobile manufacture. Companies that size can distort the market and have tremendous political influence, often greater influence with regard to their own regulation and guidance than the customers they serve—even when those customers constitute essentially the entire electorate in democratic societies.

In the United States for example, automobile manufacturers, suppliers, and dealers provide over seven million jobs,⁸⁴ and the automotive sector employed 5.6% of all EU workers in 2013.⁸⁵ In light of the significance for job markets and overall economies, governments have been known to subsidize and bail out car companies in times of trouble or to stimulate growth. Notably, the United States government provided approximately \$80 billion to the automobile industry during the 2008 economic downturn.⁸⁶ Germany invested \$1.1 billion towards subsidizing electric-powered cars,⁸⁷ and many other countries have implemented various schemes to promote electric vehicle sales, including access to express lanes, exemptions from road tolls, and reduction or elimination of taxes on fuel and vehicle registration fees.⁸⁸ As such, the automotive industry shares a uniquely deep

84. CTR. FOR AUTO. RESEARCH, CONTRIBUTION OF THE AUTOMOTIVE INDUSTRY TO THE ECONOMIES OF ALL FIFTY STATES AND THE UNITED STATES 1 (2015), <http://www.cargroup.org/wp-content/uploads/2017/02/Contribution-of-the-Automotive-Industry-to-the-Economies-of-All-Fifty-States-and-the-United-States2015.pdf>.

85. *Employment Trends*, EUROPEAN AUTO. MFRS. ASS'N, www.acea.be/statistics/tag/category/employment-trends (last visited Sept. 17, 2017).

86. Brent Snively, *Final Auto Rescue Tally: Taxpayers Lost \$9.3 Billion*, DETROIT FREE PRESS (Dec. 30, 2014, 9:43 AM) www.freep.com/story/money/cars/2014/12/30/treasury-auto-rescue-gm-chrysler-ford/21044191/. Much of the government funding has been since returned. *Id.*

87. Bruce Brown, *Germany Announces \$1.1 Billion in Subsidies for Electric Cars*, DIGITAL TRENDS (Apr. 27, 2016, 7:00 AM), www.digitaltrends.com/cars/germany-electric-car-subsidy/.

88. *Overview of Purchase and Tax Incentives for Electric Vehicles in the EU in 2016*, EUROPEAN AUTO. MFRS. ASS'N (Aug. 4, 2016), http://www.acea.be/uploads/publications/Electric_vehicles_overview_2016.pdf. China has also subsidized its electric vehicle market. Christian Shepard, *China Shifts Gears to Drive Electric Car Development*, FIN.

economic relationship with various national governments. Consequently, they have to endure a lesser degree of economic freedom than manufacturers in the information technology sector and other industries.

Most governments also intervene based on antitrust laws and competition policy to counteract market inefficiencies created by tying, monopolization, exclusionary measures, refusal to deal, and other anticompetitive strategies to close markets to effective competition.⁸⁹ It is within the purview of governments to act in the interest of the automobile customer by influencing the manufacturers to embrace more openness and maintain an independent aftermarket, indeed one that can produce autonomous driving systems for all vehicles. Just as past governments legislated for a standardized opening for car radios and a standard connector and protocol for smog testing, present governments have the power to guide automobile manufacturers to provide more open interfaces and allow for a thriving aftermarket.

2. *Cybersecurity: The Phantom Menace*

Cybersecurity is currently one of the greatest global concerns, and its potential impact on the automotive industry has not been taken lightly. Consumers, regulators, and companies are worried about the risk that criminals could manipulate connected cars by remotely taking control of on-board computers, especially those critical to passenger safety. For example, in 2015, two security researchers demonstrated that they could manipulate the transmission and shut down the engine of a Jeep while it was on the highway. The report on the research “floated around the entire federal government” including Homeland Security.⁹⁰

Public concerns about security are often used as justification for cracking down on freedoms and locking up open doors. A few years ago, a few leading information technology companies, organized as the Trusted Computing Group,⁹¹ tried to lock down personal computers in the interest

TIMES (Feb. 25, 2016), <http://www.ft.com/cms/s/0/a55e7d36-db8a-11e5-a72f-1e7744c66818.html>.

89. See *infra* Section IV.B.

90. Pete Biglow, *Feds Fretting Over Remote Hack of Jeep Cherokee*, AUTOBLOG (July 23, 2016, 10:13 PM), <http://www.autoblog.com/2015/07/23/feds-fretting-jeep-cherokee-remote-hack-exclusive/>.

91. For a full list of members of Trusted Computing Group, see *Member Companies*, TRUSTED COMPUTING GRP., <http://www.trustedcomputinggroup.org/about/member-companies/> (last visited Sept. 17, 2017).

of data and cybersecurity in an initiative broadly referred to as “trusted computing.”⁹² Their pitch to consumers and policymakers was that “trusted computing” involves providing a secure system of both hardware and a software operating system (i.e. a locked-down computer system architecture) where only trusted and authenticated software and content can be executed. In this context, the computing system is “trusted” because cryptographic keys are necessary to authenticate that programs running on the computer system with which they are communicating have not been modified by third parties, and that the computer system is effectively what it claims to be and is running the software it claims to be running.⁹³ For this system to work, the keys generally cannot be controlled by third-party servers, third-party content providers or the end-user.

Proponents of “trusted computing” claim that it will reduce vulnerability to viruses, phishing, malware, and cyberattacks, as well as making computers safer, more secure, and reliable for end-users.⁹⁴ Critics,

92. In 2002, Microsoft launched its Trustworthy Computing initiative (originally known as “Palladium” but now more commonly known as “Next-generation Secure Computing Base” (“NGSCB”). See CRAIG MUNDIE ET AL., MICROSOFT, TRUSTWORTHY COMPUTING (2002), http://download.microsoft.com/documents/australia/about/trustworthy_comp.doc; *Security Model for the Next-Generation Secure Computing Base*, MICROSOFT CORP. (2003), www.microsoft.com/resources/ngscb/documents/ngscb_security_model.doc; Bill Gates, *Bill Gates: Trustworthy Computing*, WIRED (Jan. 17, 2002, 12:00 PM), <http://www.wired.com/2002/01/bill-gates-trustworthy-computing/> (reporting an email from Bill Gates to Microsoft employees about the initiative); *Microsoft Next-Generation Secure Computing Base – Technical FAQ*, MICROSOFT CORP. (July 2003), <https://msdn.microsoft.com/en-us/library/cc723472.aspx> (offering general technical information about NGSCB). Briefly, NGSCB is a security technology for Microsoft’s Windows Platform aimed at using specially designed secure and trusted hardware and software to enhance availability, security, privacy and system integrity for its customers. *Id.* However, detractors argued that NGSCB was in effect “Traacherous Computing,” Microsoft’s attempt to impose digital rights management on its customers which would seriously hamper a customer's control over his/her computer and the content able to be accessed.

93. For an overview of the technical aspects of “trusted computing,” see generally Ross Anderson, *Cryptography and Competition Policy - Issues with ‘Trusted Computing’*, in *ECONOMICS OF INFORMATION SECURITY* (L. Jean Camp & Stephen Lewis eds., 2004).

94. See generally MUNDIE ET AL., *supra* note 92; see also Carolin Latze & Ulrich Ultes-Nitsche, *Stronger Authentication in E-Commerce: How to Protect Even Naïve User Against Phishing, Pharming and MITM Attacks*, PROC. IASTED INT’L CONFERENCE COMMC’NS SYS. NETWORKS & APPLICATIONS (2007), <http://www.latze.ch/CSNA07.pdf>. Key features of “trusted computing” include: (i) remote attestation of the hardware and software (i.e., to authenticate to a third party that the correct software is running on the correct computer system and that it is not malware, before the data, application and/or system can be processed or run); (ii) secure pathways to the user (to ensure that encrypted

however, decry that “trusted computing” policies and technical features are a double-edged sword that can secure systems not only *for* the end-user, but also *against* the end-user.⁹⁵ Moreover, “trusted computing” can be abused to enforce remote censorship, as content created using “trusted computing” systems remain under the control of the system that created it rather than the owner of the computing system on which the content is stored. Accordingly, a “trusted computing”-compliant media player may—against the wishes of the owner—identify and report “restricted content.” It can be instructed to remotely delete content that the manufacturer believes to be illegitimate. An ebook reader software company may similarly be ordered by authorities to remotely delete a publication that expresses a contrary viewpoint to that of the government.⁹⁶ Further, critics argue that “trusted computing” will increase anticompetitive monopolistic behavior as users, particularly businesses, become locked into incumbent “trusted computing” platforms. This is likely to occur due to the significant costs and practical difficulties of accessing “trusted computing” content and software from non-“trusted computing” platforms.⁹⁷

The debate over the merits and dangers of “trusted computing” polarized the industry and consumers for many years, with the controversies

data input and output from authorized locations remains private and unaltered); (iii) sealed storage of cryptographic keys (i.e., the cryptographic keys required to unseal encrypted data cannot be removed from the “trusted computing” system); and (iv) partitioned memory (data stored within curtained memory can only be accessed by the authenticated trusted application to which it belongs (e.g., the application from which it was created or saved) and not by any other application or operating system, thereby binding data and applications to a specific system). See Donald Palmer, *Understanding Trusted Computing From the Ground Up*, ELEC. DESIGN (Nov. 12, 2012), <http://electronicdesign.com/microprocessors/understanding-trusted-computing-ground>; see also Hans Brandl & Thomas Rosteck, *Technology, Implementation and Application of the Trusted Computing Group Standard (TCG)* (Sept. 2004) (unpublished manuscript), <http://www.infineon.com/dgdl/Trusted+Computing+Overview.pdf?fileId=db3a304412b407950112b416592f203e>; MICROSOFT CORP., *supra* note 92.

95. See Richard Stallman, *Can You Trust Your Computer?*, GNU.ORG (Nov. 18, 2016, 6:31 AM), <https://www.gnu.org/philosophy/can-you-trust.en.html>; see also lafkon, *Trusted Computing*, VIMEO (June 15, 2009, 11:36 AM), <https://vimeo.com/5168045> (depicting Benjamin Stephan’s 2007 lighthearted short video questioning the merits of trusted computing that won Adobe’s Design Achievement Award for Motion Graphics).

96. See Ross Anderson, *‘Trusted Computing’ Frequently Asked Questions*, U. CAMBRIDGE COMPUTER LABORATORY (Aug. 2003), <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>.

97. Anderson, *supra* note 93.

preventing any true widespread adoption, outside of the military.⁹⁸ More recently, interest in “trusted computing” has increased again due to potential uses in cloud⁹⁹ and mobile computing.¹⁰⁰ Policymakers and traditional automobile manufacturers seem inclined to view cybersecurity concerns as a reason to steer the car of the future towards a more closed design. Yet, as the experience with personal computers and “trusted computing” controversies has shown, closed systems come with significant costs and are not necessarily more secure. Locking down interfaces to promote security may prove to be a dead-end road for the closed car.¹⁰¹

3. Health and Safety

Cars can be safer if they automatically signal to each other, particularly self-driving cars or those using driver assistance technologies. This in turn requires standardized communication protocols that are open to all car

98. For a brief discussion why industry adoption of “trusted computing” has been slow, see *Defining and Selling Trusted Computing*, INFOSECURITY MAG. (Sept. 12, 2013), <http://www.infosecurity-magazine.com/news/defining-and-selling-trusted-computing/>. The US Army and Department of Defense however have supported the adoption of “trusted computing” by mandating since 2007 that all new computer assets acquired contain Trusted Platform Module technology (i.e., a chip for the processor that conforms to the Trusted Computing Group’s standard specifications for “trusted computing”) where available, for purposes of enhancing cyber security. See Memorandum from Department of Defense, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media (July 3, 2007), <https://health.mil/Policies/2007/07/03/Encryption-of-Sensitive-Unclassified-Data-at-Rest-on-Mobile-Computing-Devices>; William Jackson, *The Quest for the Holy Grail*, WASH. TECH. (Oct. 12, 2007), <https://washingtontechnology.com/articles/2007/10/12/the-quest-for-the-holy-grail.aspx>; Donald Palmer, *Changing Military Operations Demand Fail-Safe Solutions in Cyber Security*, MIL. & AEROSPACE ELECTRONICS (Sept. 1, 2012), <http://www.militaryaerospace.com/articles/print/volume-23/issue-09/opinion/changing-military-operations-demand-fail-safe-solutions-in-cyber-security.html>.

99. See generally Eghbal Ghazizadeh et al., *Trusted Computing Strengthens Cloud Authentication*, 2014 SCI. WORLD J. 1 (2014); see also Pardeep Kumar et al., *Effective Ways of Secure, Private and Trusted Cloud Computing*, 8 INT’L J. COMPUTER SCI. ISSUES 412 (2011).

100. See N. Asokan et al., *Mobile Trusted Computing*, 102 PROC. IEEE 1189 (2014); Kathleen McGill, *Trusted Mobile Devices: Requirements for a Mobile Trusted Platform Module*, 32 JOHNS HOPKINS APL TECHNICAL DIGEST 544 (2013), http://www.jhuapl.edu/techdigest/TD/td3202/32_02-McGill.pdf; Bill Ray, *Trusted Computing: It’s Back, and Already in a Pocket Near You*, REGISTER (Feb. 29, 2012, 10:12 PM), http://www.theregister.co.uk/2012/02/29/trusted_computing/.

101. For interesting and entertaining stories on threats that closed cars can pose to their owners, see CORY DOCTOROW, *CAR WARS*, <http://this.deakin.edu.au/lifestyle/car-wars> (ebook) (last visited Sept. 17, 2017).

manufacturers. The world of connected cars will require information exchanges and a certain degree of openness in the interest of safety.

But opening up cars to unlimited modification, add-ons, and updates also raises serious safety concerns. For example, if a hobbyist or independent repair shop inadvertently or deliberately disables a vehicle's airbag systems, or any malfunction indicator lights, the driver or a subsequent vehicle owner may be subjected to great risk.¹⁰²

Cars must remain as safe as practical in light of conflicting interests, such as affordability, ease of operation, and some degree of *Fahrvergnügen* (driving pleasure). Providers of parts, add-ons, and services for the open car must be subjected to health and safety requirements that are as rigorous as those regulations that car manufacturers must meet. But government authorities may find it much more difficult to enforce health and safety requirements against thousands of app providers than against a few large automakers. One challenge in this respect is multiple-use products that are not solely or even expressly marketed as automotive products, such as portable GPS receivers or DVD players. Another challenge associated with an open car environment is that it will involve many more and smaller suppliers of parts and software that may be able to offer their products directly to consumers without any control by original equipment manufacturers (OEMs). The many recalls and historic scandals relating to automotive safety¹⁰³ highlight this particularly serious policy concern. Smaller and startup technology companies will likely have less expertise and fewer resources than established automotive manufacturers to perform health and safety testing as well as ensure continuous regulatory compliance.

By opening up car designs, governments could enhance competition and reduce the possibility of failures and cover-ups by established car manufacturers, but they could also enable a wide range of less competent and responsible market participants.

102. See General Motors LLC, *supra* note 17; see also Motavalli, *supra* note 17; Charette, *supra* note 17.

103. Max Blau, *No Accident: Inside GM's Deadly Ignition Switch Scandal*, ATLANTA MAG. (Jan. 2016), <http://www.atlantamagazine.com/great-reads/no-accident-inside-gms-deadly-ignition-switch-scandal/>.

4. *Environmental Sustainability*

Governments must continue their work on sustainability by reducing emissions, hazardous substances, and waste in the automotive industry. The more open cars are, the easier monitoring of systems and emissions becomes, as evidenced by the fact that the recent emissions scandal was uncovered by an independent security researcher.¹⁰⁴ By opening up automotive computer systems to a broader ecosystem of information technology developers, policymakers can also reduce the numbers of vehicles that will be discarded due to outdated information technology systems. Closed cars are likely to become obsolete as quickly as smart phones and may be discarded as quickly if their original manufacturer does not offer adequate updates and upgrades. Increasing the effective lifetime of vehicles benefits consumers as well as the environment. From the perspective of environmental sustainability, the open car comes out clearly ahead.

5. *Consumer Protection and Prices*

Opening up automobile aftermarkets should introduce additional competition and drive down prices for parts, repairs, upgrades, and add-ons. It could also create a spike of interest and demand in open cars, which would benefit new car sales overall as well as provide an avenue for differentiation. But it is not a given that the open car will be cheaper than the closed car. If existing car manufacturers do not do well on aftermarket sales, it is possible that they have to raise prices for original cars, which they may have subsidized in expectation of revenue from locked-in car owners in aftermarkets.

6. *Innovation and Intellectual Property Protection*

The open car has the potential to attract a flurry of innovation and hordes of new innovators from various industries and backgrounds to contribute to its development and continuous improvement. Openness can also scare more traditional investors in innovation, who might fear that they cannot monetize their contributions as well in an open environment.¹⁰⁵ The U.S. Constitution contemplates—and nearly all policymakers around the world agree—that innovators should be incentivized by exclusion rights under

104. Neate, *supra* note 81.

105. See Jay Lyman, *SCO Claims Linux GPL Is Unconstitutional*, TECHNEWSWORLD (Oct. 28, 2003, 3:04 PM), www.technewsworld.com/story/31975.html; Darl McBride, *Open Letter on Copyrights*, SCO.COM (Dec. 4, 2003), www.sco.com/copyright/.

patent, copyright, trademark, and other intellectual property laws. Manufacturers that develop protectable designs, computers, and software for cars should be able to enjoy, deploy, and monetize their intellectual property rights by excluding others from infringing them. Yet, intellectual property laws are not intended to favor closed designs over open ones. The ultimate objective of intellectual property protection is to promote innovation and secure access to the best possible intellectual property for the public. Therefore, legislatures and courts have long established limits to intellectual property rights to prevent patent abuse,¹⁰⁶ misuse of copyrights,¹⁰⁷ and control of downstream distribution after a first sale,¹⁰⁸ and to protect interoperability¹⁰⁹ and keep interfaces open.¹¹⁰ The long-standing policies behind intellectual property law favor the open car.

7. *Personal Property Protection*

Like intellectual property laws, personal property laws allow property owners to exclude others. This might seem to favor closedness over openness, but only at first sight; personal property laws favor choice for the owner and not for the maker of chattels (here, the automakers). According to traditional notions of personal property, the car owner should be able to decide how the car is steered and whether it remains locked or open.

8. *Data Privacy*

Data privacy laws are intended to protect each individual's right to information, self-determination and personal privacy. One must be able to decide whether to share information about oneself or whether to keep secrets. The connected car generates immense amounts of information on its drivers, passengers, other observable traffic participants, and the environment through which it travels. Such data is of great interest to many¹¹¹: Governments can use the data to monitor traffic patterns, violations of traffic rules, automobile safety, environmental sustainability,

106. See *United Shoe Mach. Corp. v. United States*, 258 U.S. 451 (1922); see also *Int'l Salt Co. V. United States*, 332 U.S. 392 (1947).

107. *Lasercomb Am., Inc. v. Reynolds*, 911 F.2d 970 (4th Cir. 1990); 2 MELVILLE B. NIMMER & DAVID NIMMER, *NIMMER ON COPYRIGHT* § 8.12 (2013).

108. See, e.g., *Bobbs-Merrill Co. v. Straus*, 210 U.S. 339 (1908); *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013); see also 17 U.S.C. § 109 (2012).

109. See Council Directive 2009/24, Art. 6, 2009 O.J. (L 111) 19 (EC).

110. See *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 2014 (Fed. Cir. 2014).

111. David Welch, *Your Car's Been Studying You Closely and Everyone Wants the Data*, BLOOMBERG TECH. (July 12, 2016, 2:00 AM), <https://www.bloomberg.com/news/articles/2016-07-12/your-car-s-been-studying-you-closely-and-everyone-wants-the-data>.

and the whereabouts of individuals suspected of crimes and misdemeanors. Car manufacturers can use the data to monitor and enhance product safety, develop new features, improve their products, learn more about customer preferences, gain intelligence on competitors' products, and retain evidence for product liability cases. Car dealers can use the data to sell cars more effectively. Car insurance companies can develop risk profiles on particular drivers and adjust premiums and offers of insurance accordingly. Advertisers can market roadside offerings in real time or enrich unrelated consumer profiles. Fleet managers can monitor vehicle location, deployment options, driver performance, and maintenance needs.

Individual car owners, drivers, and passengers on the other hand have privacy expectations. They do not want their whereabouts and driving habits tracked by law enforcement agencies, insurance companies, employers, and others. In 2011, it was discovered that a GPS navigation device manufacturer was providing data, albeit anonymized, to Dutch government officials who used the data in part when determining where to place speed cameras.¹¹² As a result of the public outcry, the manufacturer agreed to prohibit law enforcement from using their collected data in this manner in the future.¹¹³

Car owners may or may not want information collected by their car in an accident to be used in investigations or in courts. They might accept data usage for advertising purposes in return for free services or hardware discounts—as they accept on the internet and with respect to mobile services—but they generally want to remain informed and in control.

Governments are increasingly pushing for “privacy by design” requirements on product developers. The U.S. Federal Trade Commission has brought a number of cases against product manufacturers that did not sufficiently consider data security in the design of their products, which have included network cameras,¹¹⁴ home routers,¹¹⁵ and software

112. Archibald Preuschat, *TomTom Drives Into Speed Camera Scandal*, WALL ST. J.: TECH. EUR. (Apr. 28, 2011, 6:33 PM), <http://blogs.wsj.com/tech-europe/2011/04/28/tomtomb-drives-into-speed-camera-scandal/>.

113. *Id.*

114. *See, e.g.*, Press Release, Fed. Trade Comm'n, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2014), <https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles>.

115. Press Release, Fed. Trade Comm'n, ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers' Privacy At Risk (Feb. 23, 2016),

platforms.¹¹⁶ As of May 2018, companies will be expressly required under the EU General Data Protection Regulation to consider data protection by design and by default, implement appropriate technical and organizational measures and enable data portability.¹¹⁷ Legislatures and regulators across jurisdictions can be expected to push for transparency, notice and choice regarding data also in the automotive space.

The battle for car user data may indirectly affect the open car, as strict privacy laws could inhibit data-driven business models and thus favor certain players over others in the market for open cars and associated technologies and services. But manufacturers of closed and open cars could equally focus on privacy protections for drivers and passengers with technical features, or pursue strategies to collect and commercialize user data.¹¹⁸ The connected car relies on information exchanges for safety and technical purposes, but the open car does not need to run on open data.

9. *Summary of Policy Considerations For and Against the Open Car*

Environmental sustainability, innovation, and competition considerations favor the open car. Health and safety concerns suggest heightened scrutiny, but the connected car will require information exchanges and open communication protocols. Fears about cybersecurity and data privacy do not support policies against openness, because transparency advantages outweigh benefits from relying on a few trusted manufacturers.

<https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put/>.

116. Press Release, Fed. Trade Comm'n, Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates (Dec. 21, 2015), <https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java>.

117. See Council Directive 2016/670, 2016 O.J. (L 119) (EU).

118. The European Automobile Manufacturers Associations ACEA acknowledges that data is the fuel of the digital economy and focuses on risks resulting from access to data by third parties (i.e., companies other than the automobile manufacturers). PINSENTMASON, CONNECTED AND AUTONOMOUS VEHICLES: THE EMERGING LEGAL CHALLENGES (2016), <https://www.pinsentmasons.com/PDF/2016/connected-and-autonomous-vehicles-2016.pdf>. Professor Ricardo Jackson also analyzes the value of data generated by the “connected and automated vehicles” and approaches the perspective of the “data owner, probably the vehicle manufacturer” with the assumption that car manufacturers also own all data generated by cars. *Id.* at 15.

C. POSSIBLE DEGREES OF OPENNESS FROM A TECHNICAL PERSPECTIVE

Based on the policy considerations discussed, the open car will have to be strictly regulated for health and safety reasons, but should provide the capability for aftermarket equipment to connect to its interfaces and replace some equipment. For example, a car owner should be able to add an aftermarket entertainment, navigation, or telematics system that interoperates correctly with all of the automobile's systems. The potential for an aftermarket autonomous driving system to be added is especially interesting. Allowing for the addition of such facilities requires that some components of the automobile be deliberately released without confidentiality restrictions and that they be designed to facilitate interoperability between vendors. They must be robust against error and failures such that mal-performance of the added-on part does not cause the automobile's other systems to crash. We call this level "open interfaces."¹¹⁹

Beyond open interfaces, there might be the ability for software creators to create new software to replace or run alongside of the automobile's original software. In the case of entertainment systems this means the ability to run apps from third parties, as many smartphones do. This is referred to as "open platforms."

Software and hardware designs can be publicly disclosed to make it easier for third-party security researchers to find bugs and security issues, thus abandoning trade secret status while remaining copyright protected with all rights reserved except the right to read and discuss what one has read. This avoids problems with nondisclosure agreements, the conventional method used for this sort of examination. Security researchers work most efficiently when they can cooperate with each other and discuss their findings, which in general would be prevented by nondisclosure. The public also has an interest in being informed of security flaws and bugs which affect their safety and privacy. Software source code that is disclosed but still protected by copyright is referred to as "disclosed source code." For hardware designs, the disclosure of schematics, engineering drawings, and other information can be referred to as "disclosed hardware design."

Beyond the aforesaid categories, there is "open source software."¹²⁰ Open source software is fully disclosed in the form preferred for software

119. Carol Sledge, *A Discussion on Open-Systems Architecture*, SOFTWARE ENGINEERING INST. BLOG (Nov. 23, 2015), https://insights.sei.cmu.edu/sei_blog/2015/11/a-discussion-on-open-systems-architecture.html.

120. BRUCE PERENS, OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION, (1999).

modification, and comes with intellectual property terms that allow its redistribution, modification, and use. Efficient software development and improvement involves copying and adapting existing source code, which requires permissions under copyright law. The fact that copyright law protects software code and enables authors to condition permissions on license terms that require other developers to also grant permissions to their adaptations has ensured the success of the open source software movement.

Attempts to transfer the open source software approach to inventions (“open patents”), hardware (“open hardware”),¹²¹ and data (“open data”)¹²² have been less successful because the law of patents for inventions requires expensive filings and does not allocate adaptation rights to the first inventor, and because hardware and data are not subject to copyright protection. Innovators who release inventions, hardware, or data on “open terms” may be able to impose contractual requirements of continued openness on the first tier of acquirers, but they would not have efficient remedies against downstream users who are not bound by contractual terms and do not honor openness requirements.

Given the presence and strategic importance of software in today’s cars, open source software licensing terms play an increasing role with respect to cars, but many goals and benefits of openness can be reached with open interfaces, open platforms, disclosed hardware designs, and source code disclosures.

The increasing value of technical and personal data generated by and with cars raises another dimension of openness—namely with respect to data. The connected car must exchange information with other devices and systems to deliver maps, location, traffic, news, entertainment, and other data. The autonomous car must exchange information with other cars, cyclists, pedestrians, and other traffic participants for safety purposes. Exchanging information requires giving and taking. It requires open, standardized communication protocols. The open car does not necessitate compromises regarding data privacy, but it will require additional safeguards to protect drivers, passengers, operators, and owners with respect to their personal data and privacy. Companies pursuing data-driven business models may push for open data and may offer consumers

121. John R. Ackerman, *Toward Open Source Hardware*, 34 U. DAYTON L. REV. 183 (2008).

122. *What Is Open Data?*, OPEN KNOWLEDGE INT’L, <http://opendatahandbook.org/guide/en/what-is-open-data/> (last visited Sept. 17, 2017).

compelling offerings (e.g., “free” open car for drivers who agree to give their data). But the open car does not need to run on open data.

IV. THE OPEN CAR AND CURRENT LAW

After reviewing arguments for and against the open car from a policy perspective in Part III of this Article, we will now turn to a review of currently applicable law to identify requirements, support, and obstacles for the open car, including laws on motor vehicle safety, emission controls, right to repair, telecommunication regulations, competition, intellectual property, data privacy, and product liability.

A. MOTOR VEHICLE SAFETY LAWS

The National Highway Traffic Safety Administration (NHTSA) has a legislative mandate under the Motor Vehicle Safety Act to issue Federal Motor Vehicle Safety Standards (FMVSS) which are federal regulations with which manufacturers of motor vehicles and equipment must conform and self-certify compliance.¹²³ The NHTSA can regulate any equipment that poses a safety concern, including emerging technologies introducing potential safety risks.¹²⁴ The currently-enacted FMVSS affect a broad range of subsystems within a car, including antilock braking systems (ABS), and electronic stability control (ESC),¹²⁵ and adaptive cruise control.¹²⁶ It is

123. See 49 U.S.C. § 301 (2012); 49 C.F.R. § 501 (2016); see also Request for Public Comments: Safety-Related Defects and Emerging Automotive Technologies, 81 Fed. Reg. 18935 (Apr. 1, 2016).

124. Request for Public Comments: Safety-Related Defects and Emerging Automotive Technologies, 81 Fed. Reg. 18935 (Apr. 1, 2016).

125. U.S. DEPT. TRANSPORTATION, FED. MOTOR VEHICLE SAFETY STANDARDS & REGS., Standards 101, 105, 126, <http://www.nhtsa.gov/cars/rules/import/FMVSS/> (last visited Sept. 17, 2017); see also Patrick Hubbard, *Sophisticated Robots: Balancing Liability, Regulation and Innovation*, 66 FLA L. REV. 1083, 1840 (2014); Sven A. Beiker, *Legal Aspects of Autonomous Driving*, 52 SANTA CLARA L. REV. 1145, 1146–48 (2012); Julie Goodrich, Comment, *Driving Miss Daisy: An Autonomous Chauffeur System*, 51 HOUS. L. REV. 265, 268–75 (2013).

126. A car with adaptive cruise control can automatically reduce speed, applying brakes if necessary, when the car detects an object (generally another vehicle) that is near its front. See Bill Howard, *What is Adaptive Cruise Control, and How Does It Work?*, EXTREMETECH (June 4, 2013, 2:19 PM), <http://www.extremetech.com/extreme/157172-what-is-adaptive-cruise-control-and-how-does-it-work>. This feature is often paired with a forward collision warning system. *Id.*

important to note the FMVSS merely set minimum safety performance requirements rather than dictating *design* specifications.¹²⁷

The United States does not recognize the UN regulations created by the World Forum for Harmonization of Vehicle Regulation.¹²⁸ Domestic and foreign manufacturers are required to register with the NHTSA, so long as they manufacture or import any equipment covered by an FMVSS.¹²⁹ When offering a product for sale, a manufacturer is further required to self-certify that the product meets all applicable FMVSS.¹³⁰ If a manufacturer determines that it has placed a product on the market that does not comply with FMVSS or shows a safety-related defect, it must notify the NHTSA within five days of making such determination.¹³¹

Aftermarket equipment manufacturers, sellers, dealers, and importers are also subject to the prohibition against making required safety equipment inoperative and reporting safety-related defects.¹³² A part or product is considered an “aftermarket” part if it is marketed and used either to replace an original part or as an accessory that can be added onto a car.¹³³ It is illegal to market any aftermarket part that does not conform with an applicable

127. 49 C.F.R. § 571 (1999); *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., NEW MANUFACTURERS HANDBOOK (2014), http://www.nhtsa.gov/cars/rules/maninfo/Manufacturer_Information_March2014.pdf.

128. *Recommended Best Practices for Importers of Motor Vehicles and Motor Vehicle Equipment*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (July 19, 2016), <https://one.nhtsa.gov/Laws-%26-Regulations/Recommended-Best-Practices-for-Importers-of-Motor-Vehicles-and-Motor-Vehicle-Equipment>; *see also* Stephen Edelstein, *Grey Market Cars: Everything You Need to Know to Avoid Your Ride Get Crushed*, DIGITAL TRENDS (Aug. 30, 2013, 3:00 PM), <http://www.digitaltrends.com/cars/grey-market-cars-everything-you-need-to-know/>. UN-compliant vehicles and equipment are not authorized for import, sale, or use in the United States unless they are tested to be compliant with U.S. car safety laws, or for limited non-driving use (e.g. car show displays).

129. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 128.

130. 49 C.F.R. § 571 (1999); *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 127.

131. 49 C.F.R. § 573.6 (2014).

132. 49 U.S.C. § 30122(b) (2012).

133. U.S. DEPT. OF COMMERCE, ON THE ROAD: U.S. AUTOMOTIVE PARTS INDUSTRY ANNUAL ASSESSMENT 4 (2011), <http://www.trade.gov/td/otm/assets/auto/2011Parts.pdf> (“Aftermarket parts are divided into two categories: replacement parts and accessories. Replacement parts are automotive parts built or remanufactured to replace OE [original equipment] parts as they become worn or damaged. Accessories are parts made for comfort, convenience, performance, safety, or customization, and are designed for add-on after the original sale of the motor vehicle.”).

FMVSS or would take a vehicle out of compliance with a safety standard (“make inoperative”).¹³⁴

On April 1, 2016, the NHTSA issued a draft Enforcement Guidance Bulletin noting that its jurisdiction extends to: (1) automated vehicle technologies, whether sold as part of a new vehicle or aftermarket replacement/improvement, (2) software including the programs, instructions, code, and data used to operate computers and related devices, such as mobile apps and aftermarket software updates; and (3) software that can affect the car through a remote connection (e.g. the software is run from an external server).¹³⁵ Both automakers and equipment manufacturers using new and emerging vehicle technologies and equipment are obligated to notify NHTSA of any safety-related defects.¹³⁶

The NHTSA stated in its proposed guidance that in assessing whether a motor vehicle or piece of equipment poses an unreasonable risk to safety, the NHTSA considers the likelihood of a harm occurring, the potential frequency of a harm, the severity, the known engineering or root cause, and other relevant factors.¹³⁷ Further, under the NHTSA’s interpretation of its statutory mandate, the agency could compel a recall if a “cybersecurity vulnerability in any of a motor vehicle’s entry points (e.g., Wi-Fi, infotainment systems, the OBD-II port) allows remote access to a motor

134. See 49 U.S.C. § 301.02 (2012); 49 C.F.R. § 571 (1999); see also Make Inoperative Exemptions, 79 Fed. Reg. 38792 (July 9, 2014). Repair businesses and dealers would be exempted from the prohibition to facilitate their modification of motor vehicles so that persons with disabilities can drive or ride in them.

135. See 81 Fed. Reg. 18935, 18936. NHTSA’s jurisdiction is based on the fact that under the Safety Act, NHTSA’s authority covers safety defects apply to any type of product, not just those covered by current FMVSS. Any safety-related defects due to automotive technology under the propose Guidance of the NHTSA, including cybersecurity risks, would require notification.

136. See 49 C.F.R. § 573 (2014).

137. NHTSA will weigh several factors in determining whether a vulnerability poses an unreasonable risk to safety including: (i) The amount of time elapsed since the vulnerability was discovered; (ii) the level of expertise needed to exploit the vulnerability (e.g., whether a layman can exploit the vulnerability or whether it takes experts to do so); (iii) the accessibility of knowledge of the underlying system (e.g., whether how the system works is public knowledge or whether it is sensitive and restricted); (iv) the necessary window of opportunity to exploit the vulnerability (e.g., an unlimited window or a very narrow window); and, (v) the level of equipment needed to exploit the vulnerability (e.g., standard or highly specialized). See Christopher Achatz & Ashlee Difuntorum, *Cybersecurity Issues of Self-Driving Vehicles*, BRYAN CAVE (July 17, 2017), <https://www.bryancave.com/en/thought-leadership/cybersecurity-issues-of-self-driving-vehicles.html>.

vehicle's critical safety systems (*i.e.*, systems encompassing critical control functions such as braking, steering, or acceleration)."¹³⁸

The NHTSA also considers how certain features and technologies affect driver behavior. In 2013, the agency published nonbinding guidelines which recommended automakers disable certain functions of a car's built-in infotainment systems whenever the vehicle was in motion, including avoiding 3D or photorealistic images for navigation.¹³⁹

States are free to enact further equipment regulations which adopt NHTSA's standards and their own regulations in the absence of a federal standard.¹⁴⁰ For example, the NHTSA noted in a 2016 policy statement concerning automated vehicles that any potential framework and future regulations would not bar states from setting additional standards.¹⁴¹ States are in fact leading the charge in drafting and enacting legislation to deal with emerging technologies used in vehicles, with many states having enacted legislation regulating the use of autonomous vehicles.¹⁴²

States have also started to address liability concerns and the degree of openness for automotive designs in legislation.¹⁴³ For example, under one proposed Michigan law, a manufacturer is "immune from civil liability for damages that arise out of any modification made to a motor vehicle, an automated motor vehicle, an automated driving system, or automated technology by another person without the manufacturer of automated technology's consent."¹⁴⁴ This could effectively reduce automakers' liability concerns associated with further opening up their systems to third-

138. 81 Fed. Reg. 18935, 18938 (Apr. 1, 2016).

139. NHTSA Driver Distraction Guidelines, 78 Fed. Reg. 24817, 24885-86 (Apr. 26, 2013).

140. *Id.*; see, e.g., *Our Progress*, CAL. AIR RES. BD., <https://ww2.arb.ca.gov/> (last visited Sept. 17, 2017) (discussing California's adopted regulations).

141. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN, NHTSA PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (last visited Sept. 17, 2017). The NHTSA expects to release guidelines for autonomous driving on July 2016. Bruce Brown, *NHTSA Autonomous Car Guidelines Coming By July*, DIGITAL TRENDS (June 15, 2016, 5:50 PM), <http://www.digitaltrends.com/cars/nhtsa-autonomous-vehicle-guidelines/>.

142. *Autonomous Vehicles: Self-Driving Vehicles Enacted Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Aug. 29, 2017), <http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>.

143. *Id.*

144. S.B. 997, 98th Leg., Reg. Sess. (Mi. 2016), [http://www.legislature.mi.gov/\(S\(3kyj5rcy0zfcuv0niutsaxw\)\)/mileg.aspx?page=GetObject&objectname=2016-SB-0997](http://www.legislature.mi.gov/(S(3kyj5rcy0zfcuv0niutsaxw))/mileg.aspx?page=GetObject&objectname=2016-SB-0997).

party developers.¹⁴⁵ But not all such proposals, even within Michigan, would have this effect. Michigan's Senate is also considering a bill that would make it illegal for *any* person to access an electronic system of a motor vehicle to “willfully destroy, damage, impair, alter, or gain unauthorized control” of the vehicle.¹⁴⁶ A third proposal, would amend the criminal code for computer crime involving automobiles, setting the sentence to life in prison.¹⁴⁷ Under the bill's current language even security researchers, who operate with the intention to alert the manufacturer or public of any dangerous security flaws, could receive a life sentence. The bill would also be in contradiction with the Library of Congress's newly issued exemptions for the Digital Millennium Copyright Act (DMCA) which allows circumvention of TPMs for purposes of conducting research of vehicle software flaws.¹⁴⁸

In summary, current safety standards for automobiles in the United States do not present any insurmountable obstacles to openness, but recent state legislature and federal agency initiatives have the potential to impose obligations and liability on car manufacturers that could cause these to favor more closed designs.

B. EMISSIONS CONTROLS AND OPEN PORTS

The On-Board Diagnostic-II (OBD-II) port, which currently serves as an easy access point for intra-vehicle information streams and sensor data, was actually the unique result of environmental regulations. In the 1980s, the California Air Resource Board (ARB) began a smog check program to combat air pollution.¹⁴⁹ Its goal was to identify vehicles with emissions systems in need of repair. In 1988, the ARB developed the first generation On-Board Diagnostic (OBD) requirements, which required vehicles' internal computer systems to monitor emissions performance and alert

145. For further discussion of the effects of product liability upon openness, see *infra* Section IV.H.

146. S.B. 927, 98th Leg., Reg. Sess. (Mi. 2016), [http://www.legislature.mi.gov/\(S\(da5dsv23j3nis4gwm2rnmd\)\)/mileg.aspx?page=GetObject&objectname=2016-SB-0927](http://www.legislature.mi.gov/(S(da5dsv23j3nis4gwm2rnmd))/mileg.aspx?page=GetObject&objectname=2016-SB-0927).

147. S.B. 928, 98th Leg., Reg. Sess. (Mi. 2016), [http://www.legislature.mi.gov/\(S\(da5dsv23j3nis4gwm2rnmd\)\)/mileg.aspx?page=GetObject&objectname=2016-SB-0928](http://www.legislature.mi.gov/(S(da5dsv23j3nis4gwm2rnmd))/mileg.aspx?page=GetObject&objectname=2016-SB-0928).

148. For more information on DMCA exemptions, see Maria Scheid, *New DMCA Exemptions*, OHIO ST. U. LIBR. (Dec. 30, 2015), <https://library.osu.edu/blogs/copyright/2015/12/30/new-dmca-exemptions/>.

149. See *History of the Air District*, BAY AREA AIR QUALITY MGMT. DIST. (Aug. 20, 2014), <http://www.baaqmd.gov/about-the-air-district/history-of-air-district>.

owners to possible issues.¹⁵⁰ As the technology developed, there was a desire to expand the capabilities of the On-Board Diagnostic systems. The ARB developed the OBD-II requirements to monitor nearly every component that could affect the emissions performance of a vehicle,¹⁵¹ and in 1996, the Society of Automotive Engineers (SAE) assisted in the OBD-II development process by creating a standard connector plug and set of diagnostic test signals.¹⁵²

The ARB enforced the OBD-II monitoring requirements beginning with the 1996 model year, for all vehicles sold in California, and the EPA adopted the OBD-II requirements for vehicles sold throughout the United States beginning in the same year.¹⁵³ In effect, the ARB and EPA had put in place a system that could detect pollution-causing malfunctions throughout a vehicle, alert the driver to the issue, and store specific fault codes and other relevant information about the malfunction, which could be retrieved by connecting standardized equipment to the OBD. The OBD-II requirements were already eclipsing their original intent, as they now provided a means for technicians to rapidly diagnose and repair vehicles. Dealers began using these ports to read engine diagnostic codes for everything from an engine vacuum leak to a malfunctioning emissions system.¹⁵⁴

The U.S. Environmental Protection Agency (EPA) along with state agencies such as the California Air Resources Board (CARB) continue to regulate emission-related parts.¹⁵⁵ Any part affecting motor vehicle emissions is subject to anti-tampering laws, requires testing, and must be certified, whether the installation is done by owners or a repair facility.¹⁵⁶ While it is currently permitted for an engine control unit to be replaced in

150. CAL. AIR RES. BD., *supra* note 4.

151. *Id.*

152. *On-Board Diagnostics (OBD) Program*, CAL. AIR RES. BD. (June 29, 2017), <http://www.arb.ca.gov/msprog/obdprog/obdprog.htm>.

153. CAL. AIR RES. BD., *supra* note 4.

154. *See Vehicle Emissions On-Board Diagnostics (OBD)*, ENVTL. PROT. AGENCY, www.epa.gov/state-and-local-transportation/vehicle-emissions-board-diagnostics-obd (last visited Sept. 17, 2017). Computer-based early warning system are required by the 1990 CAA and comes standard on all MY1996 and newer light-duty cars and trucks.

155. *See EPA Emission Standards Reference Guide for On-Road and Nonroad Vehicles and Engines*, U.S. ENVTL. PROT. AGENCY, <https://www.epa.gov/emission-standards-reference-guide> (last visited Sept. 17, 2017).

156. CAL. AIR RES. BD., *supra* note 152.

the aftermarket, the part must comply with standards including the OBD–II protocol, or the owner and mechanic could be subject to penalties.¹⁵⁷

Today, vehicles have become increasingly computerized, and the OBD–II (or OBD, generally) is one part of a vehicle’s communications infrastructure. The desire to expand On–Board Diagnostics’ capabilities has continued, and information regarding vehicles’ performance, operations and the status of numerous components is now accessible via the standardized connection to the OBD system.

In addition to making diagnosis and repairs more efficient, the availability of functional and operational data from the OBD system has provided for the rise of telematics, which in the case of automobiles generally refers to the use of hardware to collect, transmit and study vehicle data accessed through the OBD interface and other sensors, most likely an accelerometer and GPS. Given the wealth of information now available, being able to collect and analyze that data—both in individual cases and in the aggregate—has provided concrete benefits, especially in terms of increased safety and efficiency in fleet management.

One example of the expected gains in efficiency from telematics is found in the implementation of Executive Order 13693, which lays out federal plans for automotive sustainability. The implementation plan requires that telematics be used in federal vehicle fleets by 2017, with instructions to use telematics to collect the “maximum vehicle diagnostics” possible at the vehicle level. The plan suggests that properly utilized, telematics information can reduce fleet size, fuel use, misuse of vehicles, and both unnecessary maintenance and lack of maintenance.¹⁵⁸

The OBD interface is not just a one–way conduit from the engine to the outside world. Gaining access to an automobile’s engine control unit (ECU)¹⁵⁹ through the OBD interface to optimize performance is not uncommon in the so–called “tuner” culture. Through a process known as reflashing the ECU, tuners are able to enhance engine performance, often

157. See *Keeping Your Mod’s Warranty Intact (for Dummies)*, DUMMIES.COM, <http://www.dummies.com/how-to/content/keeping-your-mods-warranty-intact.html> (last visited Sept. 17, 2017).

158. *Implementing Instructions for Executive Order 13693, Planning for Federal Sustainability in the Next Decade*, OFFICE OF FED. SUSTAINABILITY 37–38 (June 10, 2015), (implementing § 3(g)(iii) of the Executive Order), https://www.wbdg.org/FFC/FED/EO/eo13693_instructions.pdf.

159. The acronym “ECU” is also used generically to refer to any part of the electronic system in a modern automobile.

at the cost of emissions–law compliance. Tuners use hardware interfaces such as the OpenPort 2.0¹⁶⁰ to access the ECU through the OBD–II interface, then use software such as EcuFlash¹⁶¹ to alter the parameters stored within the ECU. While such modifications generally void the manufacturer’s warranty, some manufacturers are more permissive with regard to software upgrades. In fact, Volvo offers an ECU upgrade called Polestar Performance Optimization.¹⁶² The package is software–based, installed by authorized dealers, and does not void the warranty.¹⁶³

The OBD interface provides consumers with access to other functions as well. Widely available adapters allow users to plug in to the OBD port and send data from the car to a smart phone application wirelessly using standards.¹⁶⁴ Though most available applications focus on diagnostic features such as decoding “check engine” light warnings, tracking fuel efficiency and locating a parked car,¹⁶⁵ other applications allow for more in–depth interaction with the car’s functionality. For example, one developer offers an app that allows users to remotely control many actions—including turning on the headlights, sounding the horn and unlocking the doors—on most late–model Nissan products.¹⁶⁶ Another developer offers an application that allows users to customize settings for a variety of makes and models by manipulating the car’s auto–lock and one–

160. Tactrix provides a hardware implementation of this standard. See *Tactrix Openport 2.0*, TACTRIX (Sept. 17, 2017), http://www.tactrix.com/index.php?option=com_virtuemart&page=shop.product_details&product_id=17&vmcchk=1&Itemid=53.

161. See *EcuFlash – Freedom to Tune*, TACTRIX, http://www.tactrix.com/index.php?option=com_content&view=article&id=55:image3&catid=35:iceslider (last visited Sept. 17, 2017).

162. *Model Selector*, POLESTAR, <https://www.polestar.com/intl/upgrades/model-selector/> (last visited Sept. 17, 2017).

163. See *Engineered Optimisation*, POLESTAR, www.polestar.com/intl/upgrades/optimisation/ (last visited Sept. 17, 2017).

164. See *Android Bluetooth Wireless OBDII Reader & Scan Tool - For Android Devices Only*, BAFX PRODS., www.bafxpro.com/obdreader/ (last visited Sept. 17, 2017); Dan Seifert, *Samsung’s New Dongle Gives Your Car an LTE Connection*, VERGE (Feb. 21, 2016, 6:41 AM), www.theverge.com/2016/2/21/11081476/samsung-connected-car-lte-dongle-mwc-2016.

165. *Automatic Pro*, AUTOMATIC, <https://www.automatic.com/home/> (last visited Sept. 17, 2017) (listing the homepage for the Automatic).

166. *Remote for Nissan (OBD2)*, APPLE (Mar. 14, 2016), <https://itunes.apple.com/us/app/remote-for-nissan-obd2/id821598835?mt=8> (listing the homepage for the remote for the Nissan (OBD2)).

touch window functions, turning daytime running lights on or off, and controlling a variety of other user settings.¹⁶⁷

What makes the OBD interface an effective port for controlling so many of a car's functions is the fact that it connects the user to the controller area network (CAN) bus—the network of electronic control units within the modern car.¹⁶⁸ But exposing the CAN bus to external connections can also lead to security issues. *Wired* magazine featured a demonstration by two security researchers who connected to the Wi-Fi hotspot of a 2014 Jeep Cherokee remotely through the internet, exploiting a vulnerability that allowed access through the car's IP address.¹⁶⁹ They then gained access to the CAN bus, which gave them control of virtually all of the car's functions other than steering—including cutting the transmission and slamming on the brakes.¹⁷⁰ While Chrysler was able to fix this issue relatively quickly and efficiently, the implications of improper access to these ECUs became very clear.

The OBD interface is not the only port through which a user might gain access to the CAN bus. For instance, most modern cars now feature a USB input that lets the driver connect with the infotainment system. However, the infotainment system is sometimes connected to the CAN bus, and not sufficiently firewalled. In response to public pressure generated by the *Wired* article, Chrysler recently mailed USB sticks containing a security update to patch vulnerabilities in its dashboard computer.¹⁷¹ This episode illustrates the interconnected nature of the dozens of ECUs in modern cars, and the extensive access available once one is connected to the CAN bus.

The data available through the modern OBD systems can be viewed as part of the larger trend toward the connected car. Current cars are operated largely by software, and owners and drivers now have an expectation that, as with other consumer goods, they can connect to the car through smart phones or other devices. Drivers expect and value features like hands-free

167. *Carista*, CARISTA, <http://www.caristaapp.com/> (last visited Sept. 17, 2017) (listing product homepage for Carista).

168. *ISO 11898-1:2015*, INT'L ORG. FOR STANDARDIZATION (Dec. 2015), http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63648.

169. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, *WIRED* (July 21, 2015, 6:00 AM), <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

170. *Id.*

171. Andy Greenberg, *Chrysler Catches Flak for Patching Hack Via Mailed USB*, *WIRED* (Sept. 3, 2015, 4:59 PM), <https://www.wired.com/2015/09/chrysler-gets-flak-patching-hack-via-mailed-usb/>.

calling through a car system connected to their smart phone, or the ability to route music or other entertainment from a smart phone into the vehicle.

Thus, OBD requirements originating from California environmental legislation establish an important degree of openness, which has proven essential in the context of recent emission scandals but also fostered a basis for an open development environment.

C. “RIGHT TO REPAIR” LEGISLATION AND SELF-REGULATION

To protect consumers, lawmakers have proposed or passed various statutes on the “right to repair” that require automakers to provide the same information to independent repair shops as they do to their authorized dealer network.¹⁷² Massachusetts enacted a Right to Repair bill in 2012.¹⁷³ Under such bills, car manufacturers have to open car designs to consumers and independent dealers as much as the manufacturers choose to open their designs to their own dealers, but such laws do not require car manufacturers to open ports to add-on accessories or software updates made by unaffiliated suppliers.

Even though a federal Right to Repair bill is still being considered, early in 2014, the Automotive Aftermarket Industry Association, Coalition for Auto Repair Equality, Alliance of Automobile Manufacturers, and the Association for Global Automakers signed a Memorandum of Understanding that is based on the Massachusetts law and which would commit the vehicle manufacturers to meet the requirements of the Massachusetts law in all fifty states.¹⁷⁴ Under the deal, all auto companies would make their diagnostic codes and repair data available in a common format by the 2018 model year, as the Massachusetts law requires. In return, lobbying groups for repair shops and parts retailers would refrain from pursuing state-by-state legislation.¹⁷⁵

172. See *We Are the Repair Industry*, REPAIR.ORG, <http://repair.org/association/> (last visited Sept. 17, 2017). The first bill was described as attempting to end automakers “unfair monopoly” since new technologies had given automakers the right to control the vital systems of every vehicle and any advance information repair shops needed was not provided to them.

173. *Id.*

174. Gabe Nelson, *Automakers Agree to Right to Repair Deal*, AUTOMOTIVE NEWS, (Jan. 25, 2014, 12:01 AM) <http://www.autonews.com/article/20140125/RETAIL05/301279936/automakers-agree-to-right-to-repair-deal>. The agreement included they would make available to independent repair shops the same service and training information and tools related to vehicle repair as those available to franchised dealerships.

175. *Id.*

The Coalition for Auto Repair Equality (CARE), which principally represents large auto-parts retail stores and is the primary proponent of the legislation, was unhappy with the agreement and has continued to support the bill.¹⁷⁶ Despite the significant and continued progress being made under the voluntary program, the Right to Repair measure has been reintroduced in each of the subsequent Congresses.¹⁷⁷

Right to Repair legislation and ensuing industry self-regulation are both directly focused on protecting a basic level of openness in cars. Such laws and regulations directionally support development towards the open car. But they stop short of absolutely requiring a degree of openness that would suffice to guarantee the future of the open car, because they only require OEMs to treat independent dealers like affiliated ones as well as reserving the right for OEMs to keep cars closed for everyone.

D. TELECOMMUNICATION LAW REQUIREMENTS ON CONNECTED CARS AND TELEMATICS SERVICES

To the extent that the open car will have increased (or comparable) connectivity with respect to today's vehicles, automotive manufacturers will need to remain cognizant of the telecommunications regulatory landscape. Manufacturers and aftermarket suppliers looking to develop custom communications protocols would need to be aware of restricted bands of the wireless spectrum, in both the United States and every other territory they intend to reach.¹⁷⁸ They may also benefit from bands reserved for automotive-specific use.¹⁷⁹ Cars using commercial mobile network

176. *The Coalition for Auto Repair Equality*, CARE, <http://www.careauto.org/> (last visited Sept. 17, 2017) (listing the homepage for CARE).

177. Right to Repair Act, H.R. 1449, 112th Cong. (2012).

178. *See Table of Frequency Allocations Chart*, FED. COMM'NS COMM'N (Nov. 13, 2015), <https://www.fcc.gov/engineering-technology/policy-and-rules-division/radio-spectrum-allocation/general/table-frequency#block-menu-block-4>; *see also* 47 C.F.R. 2.106 (1984).

179. In 1999, the FCC restricted a 75 MHz band around 5.9 GHz for an "Intelligent Transportation System . . . expected to improve traveler safety, decrease traffic congestion, facilitate the reduction of air pollution, and help to conserve vital fossil fuels." 14 FCC Rcd. 18221 (1999). In 2014, NHTSA approved—and has since contemplated mandating—use of this band for vehicle-to-vehicle communication directed to improving safety (*e.g.*, accident avoidance) through messages transmitted between nearby cars. *See* Press Release, Nat'l Highway Traffic Safety Admin., U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles (Feb. 3, 2013), <https://www.nhtsa.gov/press-releases/us-department-transportation-announces-decision-move-forward-vehicle-vehicle>; *see also* Press Release,

connections may soon face many of the same regulations as traditional handheld device manufacturers, including those within the Telecommunications Act of 1996, which would limit the manufacturer's ability to use or share "information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service."¹⁸⁰

Future autonomous vehicles may communicate with each other and with local infrastructure via a local radio network. Such a network could perform a similar function to turn signals or road signs, and could warn an autonomous vehicle of various hazards around it. A big problem with relying on such a network to inform autonomous driving systems is the requirement that the information be truthful. If cars and local infrastructure are made to lie about the conditions of the road and other vehicles, they could cause an autonomous vehicle to behave incorrectly (for example, stop when there is no need to) or crash. But autonomous driving systems need not be so naïve. Indeed, they will probably work most reliably when they verify all inputs against their environmental data. The potential for a system to deliberately lie on the radio link might be reason to carefully sequester the radio links and any capability to control it away from potential computer criminals. This might in turn cause authorities to tightly lock down all autonomous driving systems. There is also the potential for the link to be fed false information in the name of profit, for example to cause traffic to prefer one location (where businesses might profit from its presence) over another. However, the problematical nature of such a radio link may mean that it never becomes a practical tool for autonomous vehicles.

Manufacturers looking to increase the connectivity of their vehicles should also pay attention to consumer demands—and legislative responses—for openness and control over purchased communications

U.S. Dept. of Transp., U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology (Aug. 18, 2014), <https://www.transportation.gov/briefing-room/us-department-transportation-issues-advance-notice-proposed-rulemaking-begin>. But the future of this band is uncertain, with the FCC considering proposals to open up this band for other uses. See Michael O'Rielly, *Defining Auto Safety of Life in 5.9 GHz*, FED. COMM. COMMISSION (June 8, 2016, 12:46 PM), <https://www.fcc.gov/news-events/blog/2016/06/08/defining-auto-safety-life-59-ghz>.

180. 47 U.S.C. § 222(h)(1)(A) (2012); see also Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 679 (2015). But the FCC has historically avoided applying these regulations to vehicle communications. See *id.* at 679.

devices. In 2014, President Obama signed a bill that created the Unlocking Consumer Choice and Wireless Competition Act, noting it was “another step toward giving ordinary Americans more flexibility and choice.”¹⁸¹ In effect, it limited telecommunication providers’ actions when consumers unlocked their devices to access other telecommunication networks, though consumers could only do so for personal or intra-family use.¹⁸² As communications technology becomes increasingly embedded into vehicles, legislators and consumers may similarly demand openness from car manufacturers.

E. COMPETITION

Antitrust and competition laws are generally intended to promote openness and outlaw or limit restraints of trade. Under antitrust and competition laws, as well as self-regulatory undertakings, car manufacturers cannot monopolize aftermarkets for parts and add-on products. They have to comply with a number of rules that are designed to keep automotive markets open.

1. *Tying by Contract, Refusal to Deal or Design*

Under U.S. antitrust laws, vertical restraints are subject to a rule of reason analysis and have to be justified by pro-competitive effects on the market.¹⁸³ Attempts to close aftermarkets are generally suspect from an antitrust perspective, but the exact line between allowed and forbidden is not always clear and depends on the measures taken by OEMs, particularly if they can refer to intellectual property laws to justify exclusionary measures.

The automotive aftermarket encompasses manufacturing, remanufacturing, distribution, retailing, and installation of vehicle parts and accessories after the sale of the automobile by the original equipment

181. Bill Chappell, *Bill Allowing Americans To Unlock Cellphones Passes House, Heads To Obama*, NAT’L PUB. RADIO (July 25, 2014, 4:49 PM), <http://www.npr.org/sections/thetwo-way/2014/07/25/335351105/bill-allowing-americans-to-unlock-cellphones-passes-house-heads-to-obama>.

182. Unlocking Consumer Choice and Wireless Competition Act § 2(c), Pub. L. No. 113-144, 128 Stat. 1751 (2014).

183. J. Thomas Rosch, *Developments in the Law of Vertical Restraints: 2012*, PRACTISING L. INST. 12–17, https://www.ftc.gov/sites/default/files/documents/public_statements/developments-law-vertical-restraints-2012/120507verticalrestraints.pdf (last visited Sept. 17, 2017).

manufacturer.¹⁸⁴ Most car makers sell new cars and aftermarket parts to authorized dealers. They also supply hardware and software components to dealers to connect to cars in the services aftermarket.¹⁸⁵

OEMs can apply a variety of tools and methods to restrict aftermarket sales, including technical designs (seller can design a product that makes it difficult for the aftermarket or consumers to replace or repair), tying contracts (seller conditions the sale of a primary product with purchase of a second product or service, or a prohibition on using any other products), intellectual property licensing (seller can protect their products with design patents, utility patents, software copyrights, trademarks, and other mechanisms and refuse to license others) and price discrimination (seller offers price advantages for bundled products).¹⁸⁶ None of these approaches is absolutely prohibited, but all are subject to potential challenges under competition laws.

The law of tying has changed throughout the years. Courts have adopted the more flexible “rule of reason” to assess the competitive effects of tied sales.¹⁸⁷ Under the *Jefferson Parish* test, a per se violation in tying occurs when a seller conditions the sale of a tying product on purchase of a tied product, both are in fact separate products, the supplier has substantial power in market for the tying product, and a substantial volume of transactions are affected.¹⁸⁸ Whether a particular item qualifies as part of a car or a separate add-on product can be controversial. Some automakers are integrating GPS systems, touch screens, and safety monitoring, while they are conceding their operating systems to third parties such as Apple, Microsoft, and Google.¹⁸⁹ Also, the auto industry seems receptive to open-

184. U.S. DEPT. OF COMMERCE, ON THE ROAD: U.S. AUTOMOTIVE PARTS INDUSTRY ANNUAL ASSESSMENT 5–6 (2011), <http://www.trade.gov/td/otm/assets/auto/2011Parts.pdf>. The International Trade Administration (ITA), divides aftermarket parts into two categories: (1) replacement parts, which are built or remanufactured to replace OE parts as they become damaged, and (2) accessories, parts made for comfort, safety, or customization which are designed for add-on after the original sale of the vehicle. *Id.* at 4.

185. Norman W. Hawker, *Automotive Aftermarkets: A Case Study in Systems Competition*, 56 ANTITRUST BULL. 57, 59–60 (2011).

186. Bauer, *supra* note 64.

187. *Jefferson Parish Hosp. v. Hyde*, 466 U.S. 2 (1984); *see also* David S. Evans, *Why Do Firms Bundle and Tie? Evidence from Competitive Markets and Implications for Tying Law*, 22 YALE J. REG. 37, 46 (2005).

188. *See Hyde*, 466 U.S. at 2; *see also* Evans, *supra* note 187, at 46.

189. GM and other manufacturers have been integrating Apple software into their vehicles since 2014. *See GM Statement Regarding Apple CarPlay Integration*, GEN. MOTORS (Mar. 3, 2014), <http://media.gm.com/media/us/en/gm/news.detail.html/content/>

source platforms to maintain a competitive edge, specifically with respect to infotainment technology.¹⁹⁰ As the car becomes increasingly capable as a platform for accepting third party systems and functionality, automakers' integration practices may undergo greater scrutiny. Indeed, the development of the personal computer sparked similar governmental concerns.

In the 1990s, Microsoft acquired a dominant share of the PC operating system market and try to carry its dominance over to the emerging web browser field by bundling Internet Explorer with the Windows operating system (Windows 95).¹⁹¹ In 1997, Microsoft was sued for anticompetitive marketing practices based on the argument that Internet Explorer and Windows 95 were two self-standing products, and integrating them into one package gave Microsoft an unfair advantage over Netscape.¹⁹² Microsoft famously took the position that it had the right to bundle "even a ham sandwich" into its operating system at the time, Windows 95.¹⁹³ In 1998, the DOJ and twenty state attorneys general filed an antitrust suit against Microsoft, charging the company with abusing its market power to thwart competition. The DOJ accused Microsoft of continuing to misuse its Windows operating system by requiring PC makers to agree, as a condition of acquiring a license, to adopt a uniform "first screen" specified by

Pages/news/us/en/2014/mar/0303-apple-carplay.html; Eric Slivka, *HondaLink Offers Partial Car-iPhone Integration Ahead of Apple's 'iOS in the Car' Initiative*, MACRUMORS (Jan. 23, 2014, 11:51 AM), <http://www.macrumors.com/2014/01/23/hondalink-iphone-integration/>; Christian Zibreg, *Mercedes-Benz shows off CarPlay integration*, IDOWNLOADBLOG (Mar. 3, 2014), <http://www.idownloadblog.com/2014/03/03/mercedes-benz-apple-carplay/>.

190. See, e.g., *Daimler Advances Connected Car Technology Through Open Source and Automotive Grade Linux*, AUTO. GRADE LINUX (Jan. 5, 2017), www.automotivelinux.org/uncategorized/2017/01/05/daimler-advances-connected-car-technology-through-open-source-and-automotive-grade-linux.

191. See, e.g., James K. Sebenius, *Negotiating Lessons From the Browser Wars*, MIT SLOAN MGMT. REV. (July 15, 2002), <http://sloanreview.mit.edu/article/negotiating-lessons-from-the-browser-wars/>.

192. Carey C. Basala, *Antitrust Lawsuits Against Microsoft for Monopolizing Computer Software Markets*, SANS INST. 5 (Dec. 2001), <https://www.giac.org/paper/gsec/1579/antitrust-lawsuits-microsoft-monopolizing-computer-software-markets/101236> ("Netscape Communications Corporation charged a licensing fee to original equipment manufacturers for the use of Netscape Navigator.").

193. Rick Tetzeli & David Kirkpatrick, *America Loves Microsoft Competitors Cry Foul*, FORTUNE (Feb. 2, 1998), http://archive.fortune.com/magazines/fortune/fortune_archive/1998/02/02/237213/index.htm.

Microsoft.¹⁹⁴ Microsoft explained that the restriction was intended to “prevent OEMs from compromising the quality and consistency of Windows,” and to “ensure that all Windows users experience the product the way Microsoft intended it the first time they turn on their PC systems.”¹⁹⁵ In 1999, the trial court found that Microsoft was in violation of the Sherman Antitrust Act.¹⁹⁶ Government attorneys urged the court to split Microsoft into two separate companies as penalty for breaking antitrust laws. Ultimately, the cases settled, Microsoft changed some of its practices, and other browsers—and ultimately operating systems—gained traction.¹⁹⁷

Similarly to Microsoft in the 1990s, the auto industry and some scholars defend restraints of aftermarket parts in order to ensure equipment “quality” and protect goodwill.¹⁹⁸ For example, if a car dealer uses low quality replacement parts, then consumers might mistakenly believe the parts are made by the auto manufacturer or that the cause of the problem is the original car, not the aftermarket part, and this can harm the reputation of the car manufacturer and its products.¹⁹⁹ Confidence in the quality of non-OEM parts appears to be growing,²⁰⁰ the application of competition laws remains

194. Press Release, Dept. of Justice, Justice Department Files Antitrust Suit Against Microsoft for Unlawfully Monopolizing Computer Software Market (May 18, 1998), https://www.justice.gov/archive/atr/public/press_releases/1998/1764.htm. This sequence determines the screens that every user sees upon turning on a Windows PC. Microsoft’s exclusionary restrictions forbid, among other things, any changes by an OEM that would remove from the PC Microsoft’s Internet Explorer software or that would add to the PC a competing browser in any more prominent or visible way than the way Microsoft requires Internet Explorer to be presented.

195. Michael A. Carrier, *Unravelling the Patent-Antitrust Paradox*, 150 U. PA. L. REV. 761, 785 (2002)

196. *United States v. Microsoft*, 87 F. Supp. 2d 30 (D.D.C. 2000) (involving a set of consolidated civil actions filed against Microsoft in 1988). Violations were due to (1) Microsoft’s share of the market for Intel-compatible PC operating systems, which was extremely large and stable; (2) Microsoft’s dominant market share, which was protected by a high barrier of entry; and (3) due to that barrier, Microsoft’s customers lacked commercially viable alternative to Windows.

197. *U.S. v. Microsoft Corporation Information on the Settlement*, DEP’T OF JUSTICE (Nov. 20, 2015), <https://www.justice.gov/atrusdoj-antitrust-division-us-v-microsoft-corporation-information-settlement>.

198. See, e.g., Bauer, *supra* note 64, at 40; *Cheap Parts Can Cost You a Bundle*, CONSUMER REPORTS 15 (Feb. 1999), <http://www.eddiesautobodyct.com/cheap-car-parts-can-cost-you-a-bundle/>.

199. Bauer, *supra* note 64, at 40.

200. See U.S. DEPT. OF COMMERCE, ON THE ROAD: U.S. AUTOMOTIVE PARTS INDUSTRY ANNUAL ASSESSMENT 12 (2011), <http://www.trade.gov/td/otm/assets/auto/2011Parts.pdf> (“[M]any consumers no longer judge replacement/aftermarket parts on

controversial.²⁰¹ Some scholars favor vertical restraints because the integration of products at a single price can provide efficiencies such as marginal cost savings, quality improvements, and customer convenience.²⁰²

2. *Exclusionary Practices, Monopolization*

So long as several strong car manufacturers remain present on international markets, competition remains sufficiently strong. Monopolization challenges will therefore focus on aftermarket products for a particular brand, arguing that automotive manufacturers have monopoly power in the aftermarket for their own cars and willfully maintain such power through anticompetitive means.²⁰³ For the purposes of antitrust claims, courts have defined the relevant market as narrow as parts or repair services for a “particular brand of product or service.”²⁰⁴ Once cars are recognized as platforms (should they develop further in that direction), the analogy to an operating system—as in the Microsoft litigation of the 1990s—becomes clear. Automakers must therefore be wary to avoid willful maintenance of market power in the aftermarkets of their products through anticompetitive means. This could take the form of restricting access to key components necessary to compete in the relevant market,²⁰⁵ or the way in which an alleged monopolist integrates a software offering into its overall systems.²⁰⁶ An automaker could try to portray the safety or other benefits associated with having a more restricted system as a strong “procompetitive justification,” as customers value safety and security in their vehicles, and this could shift the burden of proof on a monopolization claim to a

anything other than form, fit, and function, since quality parts can and do come from everywhere.”).

201. *See Right to Repair: Industry Decisions and Legislative Options: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. 68 (2005) (statement of Aaron M. Lowe, Vice President of Government Affairs for the Automotive Aftermarket Industry Association) (“Dealership profits are no longer driven by new car sales alone but also parts and service revenue.”);

202. *See, e.g., Evans, supra* note 187, at 46; J. Gregory Sidak, *An Antitrust Rule for Software Integration*, 18 YALE J. REG. 1 (2001).

203. *Eastman Kodak Co. v. Image Tech. Servs.*, 504 U.S. 451, 481 (1992) (citing *United States v. Grinnell Corp.*, 384 U.S. 563, 570–571 (1966)). Some courts have included an explicit third factor that the plaintiff suffered an antitrust injury as a result. *See In re Independent Serv. Orgs. Antitrust Litig.*, 114 F. Supp. 2d 1070, 1087 (D. Kan. 2000).

204. *Eastman Kodak*, 504 U.S. at 481. Further, the *Kodak* Court found there was a “natural monopoly over the market for parts [Kodak] sells under its name.” *Id.* at 459.

205. *See id.* at 481.

206. *United States v. Microsoft Corp.*, 253 F.3d 34, 58 (D.C. Cir. 2001).

plaintiff.²⁰⁷ But automakers need to remain cognizant of the possibility of monopoly claims, especially if courts begin to view cars as platforms for accepting third-party software or hardware peripherals.²⁰⁸

3. *Warranty Voidance*

Manufacturers can discourage consumers from buying aftermarket products by threatening to void warranties in case a consumer uses parts or maintenance services from third parties or by vaguely stating in maintenance instructions that the product “requires” parts or services offered by the manufacturer or its authorized dealers.²⁰⁹

Product manufacturers are not generally required to provide any warranties to end users of their products.²¹⁰ If manufacturers choose to extend consumer warranties, they must comply with numerous requirements and prohibitions under the Magnuson–Moss Consumer Warranty Act (Magnuson–Moss Act) and various state laws.²¹¹ Specifically, under the Magnuson–Moss Act, automakers cannot require that only branded parts be used with the product in order to retain the warranty.²¹² One exception to the general ban on “tie-in” provisions is that a warrantor may include a tie-in provision if it has received a waiver from the FTC.²¹³ To get a waiver, there must be proof that one’s product will not work properly without a specified item or service.²¹⁴ Improper or incorrectly performed maintenance or repair that causes damage to original equipment may also void a warranty.²¹⁵ Although the Magnuson–Moss Act

207. *Id.* at 59.

208. *See* Carrier, *supra* note 195 (providing an in-depth conversation about the cases cited in this Section and their effects on antitrust doctrines).

209. Unif. Standards in Auto. Prods. Coal., Comment Letter on Magnuson-Moss Warranty Act Rule Review (Oct. 24, 2011), www.ftc.gov/sites/default/files/documents/public_comments/16-cfr-parts-239-700-701-702-and-703-request-comments-concerning-interpretations-magnuson-moss/00022-80831.pdf.

210. Lothar Determann & Ute Krüdewagen, *Policing Social Media*, RECORDER (Apr. 6, 2012), <http://www.therecorder.com/id=1202548286075/Policing-Social-Media>

211. *Id.*; *see also* 15 U.S.C. § 2301 (2012).

212. 15 U.S.C. § 2302(c) (2012). These are commonly referred to as “tie in provisions.”

213. *Businessperson’s Guide to Federal Warranty Law*, FED. TRADE COMM’N (May 2015), <https://www.ftc.gov/tips-advice/business-center/guidance/businesspersons-guide-federal-warranty-law>.

214. *Id.*

215. *Id.*

covers warranties on repair or replacement parts in consumer products, warranties on services for repairs are not covered.²¹⁶

The Clean Air Act goes even further than the Magnuson–Moss Act in two respects: first, the Clean Air Act requires that manufacturers of new motor vehicles or engines provide buyers with a written emissions warranty²¹⁷ whereas more generally, and under the Magnuson–Moss Act, manufacturers are free to refrain from issuing express warranties to consumers. Second, under the Clean Air Act manufacturers are not only prohibited from conditioning warranty claims on usage of branded products, as they are more generally under the Magnuson Moss Act, but the Clean Air Act also requires that manufacturers issue maintenance instructions that “shall not include any condition on the ultimate purchaser’s using . . . any component or service . . . which is identified by brand, trade, or corporate name.”²¹⁸

F. INTELLECTUAL PROPERTY LAWS

Manufacturers of cars and aftermarket parts and products can protect their patented inventions against unauthorized making, selling, or using; their software against copying, adaptation and distribution; their trade secrets against misappropriation; and their trademarks against unauthorized use in commerce to the extent that it could confuse consumers. With their focus on exclusion powers, intellectual property laws can constitute an obstacle for the open car, but in many cases not an insurmountable one. The ultimate goal of intellectual property rights is to support innovation and progress. Where exclusionary rights are counterproductive to these goals, exceptions tend to be available in the interest of public access to intellectual property. Also, market forces can use the threat of exclusionary rights to require and force openness; for example, the open source software movement has very effectively instrumentalized copyrights to spread openness in software development.

1. *Utility Patents*

As cars become more and more complex computer products, companies in the automotive sector are facing the same kind of challenges from patents

216. *Id.*

217. See 42 U.S.C. § 7541 (2012); see also Unif. Standards in Auto. Prods. Coal., *supra* note 209.

218. See 42 U.S.C. § 7541; see also Unif. Standards in Auto. Prods. Coal., *supra* note 209.

as are faced by producers of complex electronics, computers, software and telecommunications products. A few companies with large patent portfolios in any given field can wield significant powers and threaten openness. Already, companies in the automotive space are filing an ever-increasing number of patents, including many software patents related to navigation and entertainment.²¹⁹ Automakers can use patents to prohibit other companies from making aftermarket parts covered by patents. At the same time, owners of computer and software-related patents can threaten automakers and aftermarket part suppliers. Potential innovators and their investors can be deterred by the mere possibility of patent claims, given the cost of litigation. Software patents in particular are difficult to analyze, given their often broad and abstract claims.

In the United States, the threat to smaller companies of overbroad or abstract software patents has been diminished since the U.S. Supreme Court heightened the scrutiny regarding subject matter limitations in *Alice*²²⁰ and U.S. Congress offered in the America Invents Act (AIA) additional options to challenge patents before the patent office.²²¹

Also, some automakers have pledged to allow unfettered use of certain patented technologies relating to the automotive field. In June of 2014, Tesla Motors CEO Elon Musk publicly aligned his company with “the spirit of the open source movement” by announcing a new policy on patent enforcement²²² which is essentially an automatic, no-signature-required form of cross-licensing if any of Tesla’s competitors actually desire it. He promised that Tesla “will not initiate patent lawsuits against anyone who, in good faith, wants to use our technology.”²²³ Furthermore, Toyota,

219. THOMSON REUTERS, *supra* note 18. Electronics companies not traditionally associated with the auto industry dominate navigation patents, automotive brands tend to focus more heavily in patents related to infotainment. *Id.*

220. *Alice Corp. v. CLS Bank Int’l*, 134 S. Ct. 2347 (2014); *see also* 35 U.S.C. § 101 (2012).

221. Post-grant proceedings created by the AIA have resulted in invalidation of at least one claim for 86% of patents that have gone to trial under inter partes review (IPR). U.S. PATENT & TRADEMARK OFFICE, PATENT TRIAL AND APPEAL BOARD STATISTICS (2016), <https://www.uspto.gov/sites/default/files/documents/2016-5-31%20PTAB.pdf>.

222. Elon Musk, *All Our Patent Are Belong To You*, TESLA BLOG (June 12, 2014), <https://www.tesla.com/blog/all-our-patent-are-belong-you>; Clark D. Asay, *The Informational Value of Patents*, 31 BERKELEY TECH. L.J. 259, 287–93 (2016).

223. Musk, *supra* note 222.

Hyundai, Kia, and Ford have joined the Open Invention Network (OIN),²²⁴ “a defensive patent pool and community of patent non-aggression” dedicated to the protection of Linux and open source software.²²⁵ Members of OIN share their patents under an agreement that provides royalty-free, worldwide, nonexclusive, nontransferable licenses for OIN patents.²²⁶ The willingness of automakers to surrender intellectual property rights in favor of more open policies could bode well for the future of the open car.

If openness does not prevail and patent wars erupt in the auto industry like in other fields, it is possible that automakers will follow the path of cellphone makers and have to adopt essential patent license requirements on reasonable and nondiscriminatory (RAND) terms. Given the complexity of the nervous system of the modern car, such a move is hardly farfetched. However, many of the current standard setting organizations (SSOs) in the automotive field champion open interoperability standards.²²⁷ In fact, at least one industry SSO has adopted open-source software policies,²²⁸ and seemingly every major auto manufacturer works with Android Auto to support an open development model for infotainment apps.²²⁹ Furthermore, Ford and Toyota are adopting SmartDeviceLink (SDL), an open-source platform for in-vehicle software. If this spirit of openness and interoperability persists, automakers may render RAND cross-licensing agreements for software patents moot.

224. *The OIN Community*, OPEN INNOVATION NETWORK, <http://www.openinventionnetwork.com/community-of-licensees/> (last visited Sept. 17, 2017).

225. *Id.*; see also Steven J. Vaughan-Nichols, *Toyota Throws Weight Behind Linux Patent Protection Group*, ZDNET (July 18, 2016, 12:50 AM), <http://www.zdnet.com/article/toyota-throws-weight-behind-linux-patent-protection-group/>; James M. Rice, *The Defensive Patent Playbook*, 30 BERKELEY TECH. L.J. 725 (2015) (explaining the concept of defensive patent portfolios).

226. *OIN License Agreement*, OPEN INNOVATION NETWORK (May 1, 2012), <http://www.openinventionnetwork.com/joining-oin/oin-license-agreement/>.

227. See, e.g., CAR CONNECTIVITY CONSORTIUM, <http://carconnectivity.org/> (last visited Sept. 17, 2017); see also CONSUMER ELECS. FOR AUTO., <https://ce4a.de/> (last visited Sept. 17, 2017).

228. GENIVI, <https://www.genivi.org/> (last visited Sept. 17, 2017).

229. *Introducing the Open Automotive Alliance*, OPEN AUTO ALL., <http://www.openautoalliance.net/> (last visited Sept. 17, 2017); *Android Auto*, GOOGLE, <https://www.android.com/auto/> (last visited Sept. 17, 2017).

2. Design Patents

Besides utility patents, automobile manufacturers have found design-patent protection very attractive.²³⁰ The number of automobile parts protected by design patents has increased dramatically in recent years.²³¹ From 2009 to 2014, the PTO issued over 1,700 design patents to the top five automakers alone.²³² Design patent owners can enforce their patents in proceedings before the U.S. International Trade Commission (ITC) to block the importation of infringing parts²³³ and sell OEM parts at higher prices.²³⁴

Aftermarket parts makers and insurance companies have pushed legislation to reduce the period car companies can enforce design patents.²³⁵

230. In order to obtain a design patent, the U.S. Patent and Trademark Office must determine that a design meets the patent requirements: new, not obvious variant of existing designs, not solely dictated by function and clearly depicted. The PTO does not require design patents to cover the entire product. The United States recognizes thirty-five classes of protectable articles of manufacture including vehicle equipment. A single invention cannot be protected by both a design and utility patent. If it is useful, then the PTO allows for a utility patent. Only an “ornamental” design can be protected by a design patent. A functional design may receive a design patent for its ornamental appearance provided that its appearance is not driven by—that is, the appearance is not the result of—its functionality. See William T. Fryer III, Comment Letter to the U.S. Patent and Trademark Office on Pending Legislation H.R. 5638 (110th Congress, 2d Session) and Design Protection (July 14, 2008), <http://www.uspto.gov/sites/default/files/web/offices/pac/dapp/opla/comments/designstownhall/fryer.pdf>; Norman Hawker, *The Automobile Aftermarket: Crash Parts, Design Patents, and the Escape From Competition*, AM. ANTITRUST INST. (Mar. 22, 2010), http://www.antitrustinstitute.org/sites/default/files/aa%20collision%20repair%20parts%20commentary_032220101350.pdf.

231. See Tracy-Gene Durkin, *2015 IPO Report Shows Continued Growth for Design Patents*, IPWATCHDOG (Nov. 20, 2015), <http://www.ipwatchdog.com/2015/11/20/63318/id=63318/>.

232. In 2014, the five top automakers were GM, Ford, Toyota, Fiat, and Honda. *Top 10 Automakers by US Sales in 2014*, WASH. TIMES (Jan. 5, 2015), <http://www.washingtontimes.com/news/2015/jan/5/top-10-automakers-by-us-sales-in-2014/>.

233. See *Ford and LKQ Settle Patent Disputes*, AFTERMARKET NEWS (Apr. 2, 2009, 12:00 AM), <http://www.aftermarketnews.com/Item/47315/ford-and-lkq-settle-patentdisputes.aspx>.

234. Jack Gillis, Dir. of Pub. Affairs, Consumer Fed’n of Am., Remarks Before the U.S. Patent and Trademark Office Town Hall Meeting on the Protection of Industrial Designs (June 16, 2008), <http://www.uspto.gov/sites/default/files/web/offices/pac/dapp/opla/comments/designstownhall/consumerfederationamerica.pdf>.

235. See, e.g., PARTS Act, H.R. 1057, 114th Cong. (2015); PARTS Act, S. 560, 114th Cong. (2015); Access to Repair Act, H.R. 3059, 111th Cong. (2009). Senator Whitehouse

The PARTS Act was introduced in 2015 to Congress.²³⁶ The bill would reduce the period during which car companies can enforce design patents on collision repair parts from fourteen years to thirty months.²³⁷ Some of the benefits proponents point to include: (1) keeping costs down for consumers;²³⁸ (2) preserving competition; and (3) bringing United States in line with European Union and Australian law.²³⁹ Those against the bill have stated that it will lead to a stall in innovation and make Americans lose jobs since most OEMs maintain design centers in the United States to create vehicles that appeal specifically to American consumers.²⁴⁰ Previous attempts to pass similar legislation have failed and as the law currently stands, aftermarket part makers must continue making sure the parts they make look substantially different from the originals. Scholars have largely

of Rhode Island introduced essentially the same bill in the Senate. S. 1368, 111th Cong. (2009).

236. PARTS Act, H.R. 1057, 114th Cong. (2015); PARTS Act, S. 560, 114th Cong. (2015).

237. PARTS Act, H.R. 1057, 114th Cong. (2015); PARTS Act, S. 560, 114th Cong. (2015).

238. See Frederick R. Warren-Boulton, Comment Letter to the U.S. Patent & Trademark Office Town Hall Meeting on the Protection of Industrial Designs 2 (June 16, 2008), www.uspto.gov/sites/default/files/web/offices/pac/dapp/opla/comments/designstownhall/hong.pdf (“Prices from independents are, on average, 26% lower than those from OEMs [and] OEM prices . . . on those parts are already 8% lower because of competition.”).

239. See *Support the PARTS Act & Keep Auto Parts Affordable*, QUALITY PARTS COAL., <http://www.keepautopartsaffordable.org> (last visited Sept. 17, 2017); see also Hawker, *supra* note 185.

240. See, e.g., *The “Promoting Automotive Repair, Trade, and Sales Act of 2015” (“PARTS Act”): Hearing on H.R. 1057 Before the Subcomm. on Courts, Intellectual Prop. & the Internet of the H. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Kelly Burris), <http://docs.house.gov/meetings/JU/JU03/20160202/104391/HHRG-114-JU03-Wstate-BurrisK-20160202.pdf>; Ryan Davis, *Bill Introduced To Shorten Term of Auto Part Design Patents*, LAW360 (Apr. 24, 2013), <http://www.law360.com/articles/435591/bill-introduced-to-shorten-term-of-auto-part-design-patents>. The Alliance of Automobile Manufacturers wrote a letter to Congress opposing a similar bill, along with other auto industry groups urging lawmakers to oppose the bill stating, “[a]t a time when the U.S. should be seeking enhanced consumer safety through stronger enforcement of our IP laws, Congress should not enact legislation that would eliminate or weaken IP protections.” *Id.*; cf. Letter from Quality Parts Coal. to Senator Chuck Grassley & Senator Patrick Leahy (Apr. 21, 2015), <http://www.pciaa.net/docs/default-source/industry-issues/qpc-senate-letter.pdf?sfvrsn=2>.

criticized design patents and some have even called for the total elimination of design patents.²⁴¹

3. *Copyright Law*

Companies have to design aftermarket parts and products with functionality and interfaces that are compatible with software and electronic control units in cars. In order to achieve compatibility, companies have to analyze and potentially reverse engineer software in cars. This raises issues under copyright law, but is largely permissible at the end of the day.

a) Copyrightability and Exceptions

Computer programs are typically protected by copyright laws at three levels—object code, source code, and graphic user interfaces—but protection does not extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery embodied in the code.²⁴² Developers are generally permitted to copy interfaces and portions of code that must be adopted to establish interoperability with independently developed programs, either because such code is excluded from copyright protection or falls under fair use considerations.²⁴³

b) Resale and Essential Step Doctrine

Under Section 117 of the U.S. Copyright Act, lawful owners of software copies sold preinstalled on cars are entitled to copy and adapt such software copies if necessary as an essential step in the utilization of such software or for purposes of repair and maintenance. Companies that distribute software for download or on CDs have largely prevailed on their position that they only license and never sell their software copies with the effects that

241. Hawker, *supra* note 185; Sarah Burstein, *The “Article of Manufacture” in 1887*, 32 BERKELEY TECH. L.J. 1 (2017) (criticizing current design patent jurisprudence); Daniel Brean, *Enough is Enough: Time to Eliminate Design Patents and Rely on More Appropriate Copyright and Trademark Protection for Product Designs*, 16 TEX. INTELL. PROP. L.J. 325 (2008) (calling for the elimination of design patents entirely); Annette Kur, *Limiting IP Protection for Competition Policy Reasons—A Case Study Based on the EU Spare-Parts-Design Discussion*, in RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND COMPETITION LAW 313, 327 (Josef Drexl ed., 2008). The authors could not find any law review articles “in defense” of design patents.

242. 17 U.S.C. § 102 (2012).

243. See Oracle Am., Inc. v. Google Inc., 750 F.3d 1339 (Fed. Cir. 2014); see also Lexmark Int’l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004); Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992); Sony Comput. Entm’t, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000).

customers and end users never become “owners” entitled under Sections 109 (first sale doctrine) or 117 (limited protection for computer programs) of the U.S. Copyright Act.²⁴⁴ Car manufacturers have reserved the possibility to take similar positions.²⁴⁵ This could entitle car manufacturers to demand the deletion of all software copies before a car owner can resell her car and largely render the car unusable. It is not clear that car manufacturers could prevail with this position in U.S. courts, given that they indisputably sell the cars on which software copies are installed in an inseparable way. But clearly, they would likely not prevail with such a position outside the United States, where software companies have found it much more difficult to enforce restrictions even with respect to stand-alone software copies.²⁴⁶ In a decision regarding the unauthorized importation of books, the U.S. Supreme Court expressed in a dictum concerns and opposition regarding the possibility that car manufacturers should be enabled to control the resale of vehicles by asserting copyrights in software.²⁴⁷

c) Open Source Code Licenses

The automotive industry has increasingly been using open source software, particularly for navigation and entertainment systems.²⁴⁸ If subject to the typical tradeoff associated with using third party code under open source code licenses, automakers may have to tolerate that aftermarket product suppliers copy and use not only interface information, but also any other code that has to be made available under the terms of the license.²⁴⁹

244. See *Vernor v. Autodesk, Inc.*, 621 F.3d 1102 (9th Cir. 2010); see also Steven A. Heath, *Contracts, Copyright, and Confusion: Revisiting the Enforceability of ‘Shrinkwrap’ Licenses*, 5 CHI.-KENT J. INTEL. PROP. 12 (2005)

245. See *General Motors LLC*, *supra* note 17, at 12.

246. Case C-128/11, *UsedSoft GmbH v. Oracle International Corp.*, 2012 E.C.R. I-0000 (July 3, 2012).

247. *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013) (noting that cars might contain copyrighted software owned by entities other than the car manufacturer but stating “principles of fair use and implied license (to the extent that express licenses do not exist) would likely permit the car to be resold without the copyright owners’ authorization”).

248. Martin von Haller, *Self-Driving Cars and Open Source—What About GPLv3 and Anti-Tivoization?*, DIGITALBUSINESS.LAW (June 27, 2016), <http://digitalbusiness.law/2016/06/self-driving-cars-and-open-source-what-about-gplv3-and-anti-tivoization/>.

249. Under Section 6 of the GPLv3 License, for example, manufacturers of consumer products have to make available not only source code but also information necessary to modify the software on the device on which it is shipped, such as a car. However, the automakers seem to be aware of this particular clause and as a result have generally avoided

d) Circumvention of Technical Protection Measures

If car manufacturers lock down interfaces and software components with technical protection measures, makers of aftermarket parts and products face an additional hurdle to interoperability: Section 1201 of the U.S. Copyright Act, which was added in 1998 as part of the Digital Millennium Copyright Act, prohibits circumvention of technical protection measures. But the U.S. Copyright Office issued an exemption in 2015 and ruled that it is not a violation of Section 1201 of the Copyright Act if a vehicle owner circumvents technical protection measures to access computer programs that are contained in and control the functioning of cars, when circumvention is a necessary step to allow the diagnosis, repair, or lawful modification of a vehicle function.²⁵⁰

In contrast, the Copyright Office limited that exemption to exclude computer programs in ECUs that are chiefly designed to operate vehicle entertainment and telematics systems due to insufficient evidence demonstrating a need to access such ECUs, and out of concern that such circumvention might enable unauthorized access to creative or proprietary content.²⁵¹ With this exclusion, the Copyright Office sought to protect copyright owner interests in entertainment content and maps but not preclude, for example, makers of aftermarket entertainment or telematics systems from accessing other ECUs or creating their own ECUs to substitute original entertainment or telematics products, or to establish connectivity between their products and existing cars.

4. Computer Interference Laws

The Computer Fraud and Abuse Act (CFAA) and other computer interference laws²⁵² prohibit and penalize circumvention of technical

using code under GPLv3. Further, it is not clear whether a car would fit under the definition of a “consumer product” and thus making its software subject to Section 6 of GPLv3. See *GNU General Public License*, FREE SOFTWARE FOUND. (June 29, 2007), <https://www.gnu.org/licenses/gpl-3.0.en.html>; Jeremiah C. Foster, *Driven to Tears—GPLv3 and the Automotive Industry*, 7 INT’L FREE & OPEN SOURCE SOFTWARE L. REV. 29 (2015); Jonathan Corbet, *LFCS: GPLv3 and Automobiles*, LWN.NET (Apr. 24, 2013), <https://lwn.net/Articles/548212/>.

250. See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944 (Oct. 28, 2015).

251. *Id.* at 65954.

252. For example, California has passed the California Comprehensive Computer Data Access and Fraud Act (forming California Penal Code § 502), which provides it a criminal offense if one “alters, damages, deletes, destroys, or otherwise uses any data, computer,

protection measures. According to the CFAA, one may not access a computer without or exceeding authorization to obtain information.²⁵³ Such laws do not promote openness or closedness. They protect computer owners in their discretion to lock down their computers to safeguard their data and privacy like personal property laws protect a car owner's choice to lock a car. Computer interference laws give the decision on openness or closeness to the owner of the computer. They apply whether a computer has wheels or not.

Under the CFAA, the owner of a car is free to access any ECU in her car, because as the owner of the computer, she is authorized. An aftermarket parts manufacturer can purchase an original car and examine its information technology systems without fear of violating the CFAA. Thus, the impact of computer interference laws on the openness of car designs is fairly limited.

But, with respect to hosted services offered for the connected car, the impact can be much more substantial. If the manufacturer of a car or aftermarket product delivers functionality associated with a car or part online from a hosted server, which remains owned and controlled by the manufacturer, it can prohibit any car owner and competitor from accessing its server in order to reverse-engineer it to establish interoperability with other parts of services. For example, if the maker of a car or navigation system delivers map information online, then third parties could not connect to the hosted service to enrich or supplement the map information.

Operators of online services have already used prohibitions of trespass to chattels and computer abuse to prevent unwanted connectivity to their systems. For example, Craigslist, the popular classified ad posting website, was able to successfully pursue a competitor scraping its housing ads under the Computer Fraud and Abuse Act, where IP address blocking and a cease and desist letter were found to provide sufficient notice of the trespass.²⁵⁴ Facebook has similarly been successful in using the Computer Fraud and

computer system, or computer network" with the purpose of, among other things, wrongfully controlling or obtaining data. CAL. PENAL CODE § 502(c)(1) (2016).

253. 18 U.S.C. § 1030 (a)(1) (2012).

254. *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013). The case ended in a settlement favorable to Craigslist, with the trespassing party agreeing to shut down operations. Cyrus Farivar, *3taps to Pay Craigslist \$1 Million to End Lengthy Lawsuit, Will Shut Down*, ARS TECHNICA (June 29, 2015, 12:38 PM), <http://arstechnica.com/tech-policy/2015/06/3taps-to-pay-craigslist-1-million-to-end-lengthy-lawsuit-will-shut-down/>.

Abuse Act as a tool against other companies scraping its data.²⁵⁵ Even though some online services offerings functionally replace distributed computing products (such as computers with preinstalled software and software copies on CDs), computer interference laws have not yet developed the same exceptions for interoperability of software-as-a-service offerings.²⁵⁶ Thus, companies that offer online services for cars from servers they own and operate can control very tightly who may connect and who may not. Just as Linux developers had to create their own entire operating system rather than add to Windows, creators of aftermarket products may have to engineer entire new clients, applications, and servers rather than touch an auto manufacturer's server.

5. *Trademark Law*

Original equipment manufacturers can rely on trademark law to protect their brands and against consumer confusion about the origin of aftermarket parts. But trademark law is not a significant obstacle to openness. Its scope has “remained constant and limited: identification of the manufacturer or sponsor of a good or the provider of a service,”²⁵⁷ with a fair use defense that “forbids a trademark registrant to appropriate a descriptive term for his exclusive use and so prevent others from accurately describing a characteristic of their goods.”²⁵⁸ Automobile manufacturers cannot use trademark law to prevent aftermarket part suppliers from referring to original part numbers²⁵⁹ or using comparative advertising to show their

255. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016).

256. Lothar Determann & David Nimmer, *Software Copyright's Oracle from the Cloud*, 30 BERKELEY TECH. L.J. 161 (2015).

257. New Kids on the Block v. News Am. Publ'g, Inc., 971 F.2d 302, 305 (9th Cir. 1992).

258. *Id.* at 306 (citing Soweco, Inc. v. Shell Oil Co., 617 F.2d 1178, 1185 (5th Cir. 1980)).

259. See K-S-H Plastics, Inc. v. Carolite, Inc., 408 F.2d 54 (9th Cir. 1969) (holding that a competitor's use of alphanumeric symbols such as “K-4” did not constitute trademark infringement because the symbols “primary significance . . . is one of pattern and not producer”); see also Wilden Pump & Eng'g LLC v. JDA Global LLC, No. CV 12-1051 ODW (DTBx), 2012 U.S. Dist. LEXIS 155599 (C.D. Cal. Oct. 29, 2012) (holding that an OEM did not have trademark protection for their part numbers when “the part numbers [were] not source identifiers, but rather, compatibility indicators”). The party alleging infringement of a part number trademark or other descriptive trademark “has the burden of proof to show secondary meaning, and that burden is substantial.” Tenneco Auto. Operating Co. v. Kingdom Auto Parts, 410 Fed. App'x. 841, 846 (6th Cir. 2010) (holding that plaintiff did not meet their burden with respect to part numbers).

aftermarket products or parts are compatible with—or improvements over—the originals.²⁶⁰ Similarly, automobile manufacturers cannot assert their trademarks to prevent third party repair shops from advertising their proficiencies in supporting particular vehicle models.²⁶¹

6. *Trade Secret Law*

Car manufacturers can protect their technical know-how and confidential business information against misappropriation, but they cannot prevent aftermarket part makers from buying a car to reverse engineer it, identify systems architectures, assess interfaces, and develop interoperable parts or software. Taking a product apart to analyze it is not prohibited under state trade secret law or the new federal Defend Trade Secrets Act of 2016.²⁶² In Europe, reverse engineering was not generally permitted under trade secret law, yet a new EU Directive on trade secret protection will permit reverse engineering within the entire European Economic Area.²⁶³

G. DATA PRIVACY AND OWNERSHIP

The connected and autonomous car depends on extensive data sharing and processing, whether it is designed as an open or closed car. Laws regarding data privacy and ownership pose neither insurmountable obstacles, nor a mandate or support for the open car.

1. *Data Privacy Laws*

Data privacy results from “legal restrictions and other conditions, such as social norms, that govern the use, transfer, and processing of personal

260. Third-party trademarks may be used in truthful comparative advertising, as long as the use is not misleading and does not create confusion among customers. *See* *Smith v. Chanel, Inc.*, 402 F.2d 562 (9th Cir. 1968) (holding a perfume manufacturer could reference, in comparative advertising, another brand’s product that they claimed to be indistinguishable); *see also* *New Kids on the Block*, 971 F.2d at 306 (finding a company may use competitor’s trademark under fair use if the company “does not attempt to capitalize on consumer confusion or to appropriate the cachet of one product for a different one”); Jacqueline Levasseur Patt, *Not All Is Fair (Use) in Trademarks and Copyrights*, 67 INT’L TRADEMARK ASS’N BULL. (Sept. 15, 2012), [http://www.inta.org/INTABulletin/Pages/NotAllIsFair\(Use\)inTrademarksandCopyrights.aspx](http://www.inta.org/INTABulletin/Pages/NotAllIsFair(Use)inTrademarksandCopyrights.aspx).

261. *Volkswagenwerk Aktiengesellschaft v. Church*, 411 F.2d 350 (9th Cir. 1969).

262. *See* *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475 (1974) (“[T]rade secret law . . . does not offer protection against discovery by fair and honest means, such as . . . reverse engineering”); *see also* UNIF. TRADE SECRETS ACT § 1 (UNIF. LAW COMM’N 1985); Defend Trade Secrets Act of 2016, Pub. L. No. 153, 130 Stat. 376.

263. *See* Lothar Determann, Luisa Schmaus & Jonathan Tam, *Trade Secret Protection Measures and New Harmonized Laws*, 17 COMPUTER L. REV. INT’L 179 (2016).

data.”²⁶⁴ Under U.S. privacy laws, drivers, passengers, bystanders and others are protected with respect to reasonable privacy expectations. Employers have to notify their drivers if they track their driving patterns or automotive systems usage,²⁶⁵ but they are not currently prohibited or restricted in using telematics systems which are in any event more often used to track commercial vehicles than the individuals who operate them. In general, it has long been established within the United States that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”²⁶⁶ But the law treats privacy of the data that is collected by the cars systems as another matter entirely. More than 90% of new cars also include event data recorders (EDR),²⁶⁷ which serve as black boxes to record critical sensor and diagnostic data prior to collisions.²⁶⁸ The federal government enacted the Driver Privacy Act of 2015, which generally limits access to EDR data to vehicle owners and lessees and those with written consent.²⁶⁹ Further, as of January 2016, seventeen states have enacted their own statutes regulating EDR data disclosure.²⁷⁰

264. Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2059 (2004).

265. See Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1004–05 (2011) (“Employers can - and often do - destroy any actual expectation of privacy by notifying employees in painstaking detail about the existence and intrusiveness of monitoring and surveillance technologies deployed.”). But employers have successfully defended against privacy claims when the tracked vehicles were company-owned, particularly in cases where the tracking was to determine employee misconduct. See Karla Grossenbacher, *Employee GPS Tracking - Is It Legal?*, LEXOLOGY: THE GLOBAL PRIVACY WATCH BLOG (Jan. 26, 2016), <http://www.lexology.com/library/detail.aspx?g=a94fd053-3106-4836-bc9c-a25d05340ed5>.

266. *United States v. Knotts*, 460 U.S. 276, 281 (1983); see also *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (“A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.”).

267. Martin Kaste, *Yes, Your New Car Has A ‘Black Box.’ Where’s The Off Switch?*, NAT’L PUB. RADIO (Mar. 20, 2013, 4:46 PM), <http://www.npr.org/sections/alltechconsidered/2013/03/20/174827589/yes-your-new-car-has-a-black-box-wheres-the-off-switch>.

268. *Privacy of Data from Event Data Recorders: State Statutes*, NAT’L CONFERENCE OF STATE LEGISLATURES (Dec. 12, 2016), <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx>.

269. Fixing America’s Surface Transportation Act §§ 24301–35, Pub. L. No. 114-94, 129 Stat. 1312 (2015).

270. NAT’L CONFERENCE OF STATE LEGISLATURES, *supra* note 268.

But EDRs are not the only tool for data collection within a vehicle; vehicles are also equipped to send data wirelessly to the automakers and third parties (e.g. for diagnostic purposes).²⁷¹ Given the privacy implications, automakers in the United States—as well as some abroad—have proactively created a set of consumer principles that guide and limit data transmission, including transparency (e.g., through providing notice of the types of data being collected), choice (e.g., requiring affirmative consent before providing certain types of data to third parties or for marketing purposes), and consumer access.²⁷²

The U.S. federal government is also considering creating a formal system of protection that is aligned with these goals, through the SPY Car Act. The associated bill was introduced to Congress in 2015 and, if enacted, would require the NHTSA and the FTC to establish consumer data privacy and car computer network security rules to prevent computer criminal access in all motor vehicles manufactured for sale in the United States.²⁷³ Further, in October 2015, House Representatives issued a memorandum suggesting legislation to require auto manufacturers to: develop and implement a privacy policy regarding the collection, sharing and use of driver and vehicle data; file their privacy policies with the Secretary of Transportation; retain data only for legitimate business purposes; and implement reasonable security measures to prevent computer crime.²⁷⁴ The proposed legislation would also impose penalties of up to \$1 million on automakers that fail to file a privacy policy or comply with an express privacy policy and fines of up to \$100,000 for failing to prevent computer crime.²⁷⁵ The proposed legislation would also require the NHTSA to create an Automotive Cybersecurity Advisory Council to develop cybersecurity best practices for vehicle manufacturers.²⁷⁶

271. *See supra* Section IV.B.

272. *See Privacy Principles for Vehicle Technologies and Services*, AUTO ALLIANCE, <http://www.autoalliance.org/auto-issues/automotive-privacy/principles> (last visited Sept. 17, 2017).

273. SPY Car Act of 2015, S.106, 114th Cong., 1st Sess. (2015). The SPY Car Act was based on a February 2015 report by Senator Markey, who had surveyed automakers about cybersecurity threats to safety and the collection and storage of driving data. The report found identified several purported weaknesses in the security of connected features in cars.

274. Memorandum from Committee Majority Staff, U.S. House of Representatives Comm. on Energy & Commerce (Oct. 19, 2015), <http://docs.house.gov/meetings/IF/IF17/20151021/104070/HHRG-114-IF17-20151021-SD002.pdf>.

275. *Id.*

276. *Id.*

EU lawmakers have already taken broad action to protect data privacy, enacting legislation that prohibits companies from processing any personal data unless they can claim a statutory exception.²⁷⁷ The term “personal data” is defined broadly as “any information relating to an identified or identifiable natural person,”²⁷⁸ which will usually include vehicle location data if someone (e.g., the car owner, lessee, employer, passenger, or others) can identify the driver. The term “processing” is also defined broadly as:

[A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[.]²⁷⁹

Such a broad definition will usually include much of what companies or governments interested in personal data want to do with it.

Yet, regarding vehicle data, companies can rely on many exceptions under EU data protection laws: in most scenarios, companies can obtain voluntary consent from drivers,²⁸⁰ for example, at the time of purchase, when consumer enable new information technology features, or by real time notices communicated via GPS systems in rental cars. Employers cannot rely on employee consent in some jurisdictions if they require all employees to accept tracking, because such consent may not be considered voluntary and could be revoked at any time.²⁸¹ But employers and providers of online services can often rely on a need to perform contractual obligations vis-à-vis the data subject, as telematics solutions and online services require data collection in order to function. Also, companies can justify data processing based on legitimate interest considerations in the EU.²⁸²

One potential concern regarding to the open car could be that it could be harder for drivers and passengers to understand and monitor the data processing practices of multiple suppliers involved in providing the open car as opposed to checking on one OEM providing a proprietary car. But

277. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 6, 2016 O.J. (L 119) 1 [hereinafter GDPR].

278. *Id.* art. 4.

279. *Id.*

280. *Id.* art. 6(1)(a).

281. *Id.* art. 7(3).

282. *Id.* art. 6(1)(f).

consumers are already used to dealing with multiple providers with respect to a much smaller yet more privacy-relevant product—their smartphones—and application platform providers have developed effective permission and disclosure systems under encouragement from the California government that could be ported to the automotive sector.²⁸³ Also, even if car manufacturers pursue proprietary, closed design and business models, they will likely pursue data commercialization plans, whether alone or with partners,²⁸⁴ and not necessarily prove more trustworthy than information technology companies with established data processing reputations and infrastructures.

2. *Data Ownership*

People sometimes get the idea that they own personal data about themselves,²⁸⁵ perhaps due to oversimplified privacy advocacy²⁸⁶ and proposals for property law regimes to protect privacy.²⁸⁷ The fact is, however, that no one owns facts. Factual information is largely excluded from intellectual property law protection: copyright law protects only creative expression, not factual information.²⁸⁸

283. See LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW ch.6-3:2 (forthcoming 2d ed. 2017).

284. See EUR. AUTO. MFRS. ASS'N, ACEA STRATEGY PAPER ON CONNECTIVITY (2016), https://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf.

285. Cf. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1130 (2000) (discussing, then refuting, reasons why individuals might naturally assume they own data about themselves).

286. See frequent references to “your own data” in press releases by the European Commission in the context of its new regulatory proposals, e.g., EUROPEAN COMM'N, HOW WILL THE DATA PROTECTION REFORM AFFECT SOCIAL NETWORKS? (2015), http://ec.europa.eu/justice/data-protection/files/3_social_network_en.pdf.

287. See, e.g., Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004); Lawrence Lessig, *Privacy as Property*, 69 SOC. RES. 247 (2002).

288. See, e.g., 17 U.S.C. § 102(b) (2012) (“In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery”); *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340, 347–48 (1991) (holding that “all facts – scientific, historical, biographical, and news of the day” are part of the public domain and are not copyrightable because they do not owe their origin to an act of authorship as required by Article I, § 8, clause 8 of the U.S. Constitution for protection) (citations omitted).

Companies that invest significant time and efforts into the creation of databases can claim limited protection under European database laws²⁸⁹ and U.S. state laws on appropriation.²⁹⁰ However, the law protects only their investment in the creation of a database, not individual bits of information within it. A manufacturer of a car or computer that stores data does not own the stored data, because the manufacturer did not create the database. A driver who causes their car's onboard computer to collect and store data does not typically own the data either, because the driver does not invest into database creation as required by database protection law. Providers and users of online services for cars, however, could create databases in which they can claim data ownership, such as map data generated via navigation systems, truck fleet management pattern data compiled via telematics services, or driver behavior information collected via driver assistance systems. Even without investing into the creation of a protectable database, companies can claim trade secret protection for information that companies develop or acquire under confidentiality obligations and keep secret with reasonable means.²⁹¹

As discussed above, many of the state statutes regulating disclosure of automotive data are in the context of event data recorders. The majority of these EDR statutes focus on disclosure restrictions rather than ownership.²⁹² However, five state statutes broach the issue of data ownership.²⁹³ For

289. Commission Directive 96/9/EC of March 11, 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) (offering copyright-like protection to creators of valuable databases).

290. *See, e.g.*, *Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841, 852–54 (2d Cir. 1997) (discussing the merits of a “hot news” misappropriation claim in the context of the unauthorized electronic delivery of near-real-time professional basketball statistics); *United States Golf Ass'n v. Arroyo Software Corp.*, 69 Cal. App. 4th 607, 611–12, 618 (1999) (discussing California's common law misappropriation as applicable to the unauthorized use of golf handicap formulas that were developed through intensive data collection and analysis); *Bd. of Trade City of Chi. v. Dow Jones & Co.*, 439 N.E.2d 526, 537 (Ill. App. Ct. 1982) (applying Illinois' common law misappropriation to the unauthorized use of the Dow Jones Index and Averages as a trading vehicle); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (AM. LAW INST. 1995); Jane C. Ginsburg, *Copyright, Common Law, and Sui Generis Protection of Data-Bases in the United States and Abroad*, 66 U. CIN. L. REV. 151, 157 (1997).

291. *See, e.g.*, CAL. CIV. CODE § 3426.11 (2016).

292. NAT'L CONFERENCE OF STATE LEGISLATURES, *supra* note 268.

293. These states are Arkansas, North Dakota, New Hampshire, Virginia and Oregon. *See* Frederick J. Pomerantz & Aaron J. Aisen, *Auto Insurance Telematics Data Privacy and Ownership*, 1 MEALEY'S DATA PRIVACY L. REP. 1 (2015), www.goldbergsegalla.com/sites/default/files/uploads/FJP-AJA_MealeysDataPrivacy_May2015.pdf.

example, Arkansas's EDR statute provides exclusive ownership of this data to the owner(s) of the motor vehicle and generally prohibits involuntary transfer of this ownership right, particularly to lienholders and insurers.²⁹⁴ The statute closely associates this data ownership with the right to consent to retrieval and use of the collected data.²⁹⁵ Oregon's corresponding statute also provides for exclusive ownership and consent rights to this data.²⁹⁶ But both statutes relate to the ownership of EDR data only, and the ownership of other types of data collected within vehicles is much less clear.²⁹⁷

H. PRODUCT LIABILITY

Car manufacturers will be more likely to oppose the open car if they are held indiscriminately liable for all defects and risks associated unsafe consumer or aftermarket modifications. This concern is real: the most recent restatement on product liability states "foreseeable product misuse, alteration, and modification must be considered in deciding whether an alternative design should have been adopted,"²⁹⁸ which suggests that car manufacturers are not shielded merely because they themselves do not create a defect causing harm. Further, certain U.S. state courts have found manufacturers liable for failing to warn users of danger stemming from post-sale modifications.²⁹⁹

Not all "misuse, alteration, and modification" is foreseeable or reasonable such that the car manufacture would be liable. In one commonly-referenced case, the New York high court discussed this threshold and found a manufacturer to not be liable due to "subsequent modification which substantially alter[ed] the product and [was] the proximate cause of plaintiff's injuries."³⁰⁰ Here, the manufacturer sold a

294. ARK. CODE ANN. § 213-112-107(c) (2010); § 213-112-107(e) (2010).

295. *Id.*

296. ORE. REV. STAT. § 105.928

297. *See Pomerantz & Aisen, supra* note 293.

298. RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY § 2 cmt. p (AM. LAW INST. 1998); *see also* Rodriguez v. Besser Co., 115 Ariz. 454, 565 P.2d 1315 (Ariz. Ct. App. 1977) ("When a product is safe for use as intended, a manufacturer has no duty to warn of dangers inherent in its use in an improper or unlikely manner, including unforeseen alterations or modifications of the product.").

299. *See* KENNETH ROSS, AM. BAR ASS'N, POST-SALE DUTY TO WARN 9 (2004).

300. Robinson v. Reed-Prentice Div. of Package Mach. Co., 49 N.Y.2d 471 (N.Y. 1980); *see also* Rodriguez, 115 Ariz. at 460 ("We believe that extending a manufacturer's duty to warn to situations in which it is notified that a third party has modified its product, after the product has left its possession and control and without consultation or participation in the modification by the manufacturer, would place an intolerable burden on the

plastic molding machine that a user subsequently modified so as to compromise a safety mechanism.³⁰¹ The court stressed that while a manufacturer may be liable for unintended yet reasonably foreseeable uses, this duty “does not extend to designing a product that is impossible to abuse.”³⁰² Courts have similarly been reluctant to find a car manufacturer at fault when a user repurposed a car component, however modularly designed it was, for a new and unexpected use.³⁰³ In an analogous context of self-driving vehicles, critics are similarly wary of placing too much liability on manufacturers, because of the risk that innovation will be stifled.³⁰⁴

A manufacturer can only be found liable under a “failure to warn” theory for product issues stemming from aftermarket products and software whose installations were reasonably foreseeable. Also, plaintiffs can bring claims on a “design defect” theory and argue that their harm was caused the original open design rather than the modifications made by the plaintiffs or third parties.³⁰⁵ If car manufacturers are held responsible for defects caused

manufacturer.”). *But see* *Liriano v. Hobart Corp.*, 92 N.Y.2d 232 (N.Y. 1998) (holding that “manufacturer liability for failure to warn may exist in cases where the substantial modification defense would preclude liability on a design defect theory,” and remanding to lower court for fact-based determination of whether meat grinder manufacturer was liable under this theory for harm caused when after meat grinder safety mechanism was removed).

301. *Robinson*, 49 N.Y.2d at 476–77.

302. *Id.* at 480–81.

303. *See Trotter v. Hamill Mfg. Co.*, 143 Mich. App. 593 (Mich. Ct. App. 1985) (holding a car manufacturer not to be liable when a user repurposed a seatbelt assembly from the manufacturer’s product to a dune buggy, noting that had they ruled the other way, the “duty would run on ad infinitum, in steering wheels, on rearview mirrors, [and] anything potentially . . . that could be pried or cut or welded off, would be potentially a target for a lawsuit, should someone be injured”).

304. Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J.L. & POL’Y 339, 362–63 (2015).

305. *See Cox v. Gen. Motors Corp.*, 514 S.W.2d 197, 200 (Ky. 1974) (“It was necessary for the parties to introduce evidence that the wheel came off the automobile as a proximate result of a design defect and not as a result of the subsequent mishandling and modification.”); *see also C & S Fuel, Inc. v. Clark Equip. Co.*, 552 F. Supp. 340, 346 (E.D. Ky. 1982) (“[T]he courts should give the defendant the benefit of a doubt where the design it did provide has been tampered with in a significant way. The policy underlying this approach is that a supplier should be strictly liable only for its own design, not for someone else’s.”); JOHN S. ALLEE, THEODORE V.H. MAYER & ROBB W. PATRYK, *PRODUCT LIABILITY* § 8.04 (2015). It may be noted that the burdens are shifted in the warranty context, where the car manufacturer must prove any problems stemmed from an installed aftermarket product before denying coverage for repairs. *Auto Warranties & Routine Maintenance*, FED. TRADE COMM’N (May 2015), <https://www.consumer.ftc.gov/articles/0138-auto-warranties-routine-maintenance>.

by aftermarket products made by unaffiliated third parties, manufacturers may be driven to close interfaces to reduce risks.

To promote openness, courts should allocate product liability on the makers and sellers of aftermarket parts and products, not the original manufacturers. This will not only require adjustments regarding substantive liability principles, but also burden-of-proof considerations, as the sheer cost of having to litigate facts relating to harm causation involving multiple product suppliers associated with open cars may justly horrify car manufacturers. It remains to be seen whether special legislation will be necessary to immunize car manufacturers from liability for aftermarket parts for the open car. Congress granted special liability privileges to online service providers in the 1990s, to promote openness and address fears of contributory liability for third party content that could have throttled freedom of information on the Internet.³⁰⁶ Congress also enacted special liability privileges for manufacturers of general aviation planes and firearms and similar privileges have been demanded for open robotics.³⁰⁷ Some states have already enacted statutes specifically to preclude manufacturer liability for harm resulting from certain modifications such as self-driving conversion kits,³⁰⁸ but the open car is not yet shielded on all roads in the United States.

306. See 47 U.S.C. § 230 (2012); 17 U.S.C. § 512 (2012); ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 55; Zittrain, *The Generative Internet*, *supra* note 55; LOTHAR DETERMANN, KOMMUNIKATIONSFREIHEIT IM INTERNET [FREEDOM OF COMMUNICATIONS ON THE INTERNET] 589 (1999).

307. See Calo, *supra* note 55; see also M. Ryan Calo, *Robotics in American Law* (Univ. of Wash. Sch. of Law Research Paper No. 2016-04, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737598. The General Aviation Revitalization Act is still in force. See *Sikkelee v. Precision Airmotive Corp.*, 822 F.3d 680 (3d Cir. 2016). Robotics-specific liability privilege legislation does not seem to have been enacted widely yet, but the sector seems to be doing quite well, judging, for example, by the list of open source robotics projects on Wikipedia. See *Open-Source Robotics*, WIKIPEDIA (last visited Sept. 17, 2017), https://en.wikipedia.org/wiki/Open-source_robotics.

308. See FRANÇOISE GILBERT & RAFFAELE ZALLONE, CONNECTED CARS RECENT LEGAL DEVELOPMENTS (2016), http://robots.law.miami.edu/2016/wp-content/uploads/2015/07/GILBERT-ZALLONE-Connected-Cars-REVISED_2016-03-29.pdf; see also S.B. 663, 97th Leg., Reg. Sess. (Mi. 2013); Assemb. Amend. to S.B. 313, 77th Sess. (Nev. 2013).

V. CONCLUSIONS AND OUTLOOK: QUO VADIS, OPEN CAR?

The tale of two cars, one open, one closed, is bound to reach its next chapter soon.

To qualify as an open car, an automotive product must be open for technology upgrades, aftermarket products and security researchers. It must have open interfaces and openly disclosed software and hardware. It will thrive if it is associated with open developer platforms. The open car does not need to run on open data. It can protect data privacy and security as well or better as proprietary automotive products do today. It does not need to run on open source software either.³⁰⁹

The closed car remains controlled by its original manufacturer, which is in most cases a large company with a strong brand, good safety track record, well-capitalized, subsidized or supported by governments, and generally considered more trustworthy than many smaller companies. The original manufacturer of a closed car retains the power to decide if and when updates and upgrades are offered for the closed car, with what functionality, and at what price. Owners of closed cars will have less options and may have to discard an automobile with a fine motor and design if its original manufacturer does not offer updates that are attractive, reasonably priced or perhaps even necessary from a safety perspective in the rapidly evolving world of connected, autonomous cars.

Either car may be the best of cars or the worst of cars. Compared to the closed, proprietary car, the open car comes out ahead based on technology, competition, sustainability and environmental policy considerations. Its enemies are citing concerns regarding cybersecurity, safety and data privacy; but upon closer review, risks in these areas do not truly justify roadblocks for open cars and rather support increased openness.

Current law is not holding the open car back. Right-to-repair statutes and competition laws are providing tailwind. Intellectual property laws do not present any insurmountable obstacles to openness. Automotive product and safety rules have not (yet) dictated a path in either direction, open or closed. On-board diagnostic ports—originally required in the interest of emission control by the California government—have become a gateway to openness and transparency.

309. But, the open car will likely run better on open source software, judging by the fact that many cars already run open source software today.

Traditional automakers seem open to embrace business models involving open platforms and standards. They have been carefully observing business models that information technology companies have successfully introduced with respect to personal computers, smartphones and other connected devices. Computers on wheels must increasingly interact and compete with other computers. Traditional car manufacturers rightfully perceive information technology companies to become their biggest competitive challenge.

But product liability concerns and the phantom menace of cybersecurity will create hurdles if manufacturers of open cars are held responsible for risks created by third party software or parts. Automakers may be reluctant to open their products further—or even decide to lock products down—if they are indiscriminately held responsible for cyberattacks and other harm created by open cars or if the sheer burden of litigation and proof becomes too threatening.³¹⁰ Sector-specific legislation and regulation may be required if courts take a wrong turn in this respect.³¹¹ Car manufacturers are rightfully concerned about excessive liability for third party actions and omissions under current product liability law. If such concerns manifest themselves in mass litigation campaigns or regulatory guidance, automobile manufacturers may turn into lock-down mode. Thus, courts and other lawmakers should carefully reconsider liability principles and precedents in the automotive, PC and Internet sectors to develop an appropriate regime regarding allocation of liability and burden of proof for defective open cars. Such regime should accept that open cars cannot be expected to be completely bug-free, just like computers without wheels are not, and shift risks associated with post sale modifications wholly or partially to the parties making the modification or the general public via insurance. Liability under “failure to warn” should be severely narrowed, as manufacturers choosing to design cars as open platforms cannot track every modification—and certainly not every combination of modifications—that consumers may choose. The law must play its role to help make the open car the best of cars.

310. See EUR. AUTO. MFRS. ASS'N, *supra* note 284, at 6 (“Vehicle manufacturers are unable to accept automatic (incalculable) liability for applications developed by third parties.”).

311. See *supra* Section IV.E; *cf.* Calo, *supra* note 55, at 601 (noting that the uncertain state of legal liability presents a similar hurdle for making more “open” robots).