Forthcoming, 32 BERKELEY TECH. L.J. Issue 2 (2017)

OPEN CARS

Lothar Determann[†] *and Bruce Perens*[††]

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 Linux[1] 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]

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, we will tell 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 or recommendation regarding the degree of openness for future cars. Rather, we intend 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.

In Part II, we provide an overview regarding the current state of automotive technology and concepts of openness in business models, technology and law. In Part III, we introduce the enemies of the open car, examine policy considerations for and against openness, and then formulate requirements regarding openness for the open car. In Part IV, we analyze how current law and regulatory mechanisms accelerate or provide road blocks for open and closed cars. We then summarize our conclusions in Part V.

---

† 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 and practices technology law as a partner with Baker & McKenzie LLP in Palo Alto, 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 [ ].

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

2 Robert Silva, *What You Need to Know About DVD Region Codes*, ABOUT TECH (updated Jan. 13, 2016), http://hometheater.about.com/cs/dvdlaserdisc/a/aaregioncodesa.htm (last visited Sept. 12, 2016).

II. CARS AND OPENNESS: NEW PATHS AND CROSSROADS

A. COMPUTER ON WHEELS

Today's premium automobiles increasingly assist and even override the driver with systems called "lane assist"[3] "summon"[4] "collision avoidance"[5] and even "autopilot."[6] Computerized systems that assist the driver in avoiding skids during braking are required of all new vehicles in the U.S. and EU[7]. Computers that manage a vehicle's conformance to pollution emissions standards[8] have been required since the 1980s.

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, transporting children under the *orders* of their parents without any adult's presence, conveying intoxicated individuals safely[9] 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.[10]

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. 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.

The modern car has been dubbed "computer on wheels,"[11] 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 multi-processor *networks* of dozens of small computers which each control a different subsystem and communicate across the rest of the vehicle via two or more

3 *Lane Assist*, VOLKSWAGEN INTERNATIONAL, http://en.volkswagen.com/en/innovation-and-technology/technical-glossary/spurhalteassistentlaneassist.html (last visited Sept. 11, 2016).

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

5 John Linkov, *Collision-Avoidance Systems Are Changing the Look of Car Safety*, CONSUMER REPORTS, Dec. 17, 2015, http://www.consumerreports.org/car-safety/collision-avoidance-systems-are-changing-the-look-of-car-safety/ (last visited Sept. 12, 2016).

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

7 *Electronic Stability Control*, NHTSA, http://www.safercar.gov/Vehicle+Shoppers/Rollover/Electronic+Stability+Control (last visited Sept. 12, 2016).

8 *Frequently Asked Questions (FAQ) About On-Board Diagnostic II (OBD II) Systems*, CALIFORNIA AIR RESOURCES BOARD, https://www.arb.ca.gov/msprog/obdprog/obdfaq.htm (last visited Sept. 12, 2016).

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

10 Jay Samit, *Driving Your Car Will Soon Be Illegal*, TECHCRUNCH, http://social.techcrunch.com/2015/08/11/driving-your-car-will-soon-be-illegal/ (last visited Sept. 12, 2016).

11 David Sedgwick, *Cars Become Computers on Wheels*, AUTOMOTIVE NEWS, Apr. 21, 2014, www.autonews.com/article/20140421/OEM06/304219993/cars-become-computers-on-wheels.

private on-board networks. At least one on-board network, often a *CAN bus*[12] (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 bus*[13] (for Media-Oriented Systems Transport), handles driver and passenger entertainment.[14]

B. ECONOMIC VISIONS OF CARS AND AUTOMOTIVE BUSINESS MODELS

Consumers select the make and model of automobile increasingly focused on information technology features: telematics, driver assistance, autonomous driving, connectivity, entertainment and various safety features.[15] 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.[16] Social media companies may push for a socially connected car,[17] 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.[18] Traditional car manufacturers may continue to focus on driving enjoyment (which Volkswagen famously marketed as "Fahrvergnügen"[19]) rather than electronic distractions.

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.

---

12 Marco Di Natale, *Understanding and Using the Controller Area Network*, 2008, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.512.5543&rep=rep1&type=pdf.

13 *MOST - Media Oriented Systems Transport*, MOST COOPERATION, http://www.mostcooperation.com/ (last visited Sept. 19, 2016).

14 *See* Comments of General Motors LLC to U.S. Copyright Office re. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07, March 27, 2015, p. 6, www.copyright.gov/1201/2015/comments-032715/; *see also* Jim Motavalli, *The Dozens of Computers That Make Modern Cars Go (and Stop)*, THE NEW YORK TIMES, Feb. 4, 2010, www.nytimes.com/2010/02/05/technology/05electronics.html; Robert N. Charette, *This Car Runs on Code*, IEEE SPECTRUM, Feb. 9, 2009, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

15 Thomson Reuters, *The State of Innovation in the Automotive Industry 2015*, http://ip-science.thomsonreuters.com/ip/SOI-Automotive-Industry-Report.pdf (all URLs in this article last accessed July 10, 2016 unless otherwise noted).

16 *Car Data: Paving the Way to Value-Creating Mobility*, MCKINSEY&COMPANY ADVANCED INDUSTRIES, https://www.mckinsey.de/files/mckinsey_car_data_march_2016.pdf (last visited Sept. 12, 2016).

17 Richard Viereckl, Jörg Assmann, and Christian Radüge, *In the Fast Lane: The Bright Future of Connected Cars*, STRATEGY& PWC (formerly BOOZ AND ALLEN), http://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf (last visited Sept. 12, 2016).

18 Nuance Launches Next-Generation Dragon Drive to Transform Connected Car with New Content, Application and Services Delivery Platform, http://www.nuance.com/company/news-room/press-releases/Nuance-Dragon-Drive-2-0.docx. (last visited Sept. 12, 2016).

19 ClassicCommercials4U, *Volkswagen Fahrvergnugen Ad from 1990*, https://www.youtube.com/watch?v=eOnne-90CLI (last visited Sept. 12, 2016).

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. It's not yet known whether future automobiles can profitably share the role of digital assistant with a more personal device[20]. Vehicles will supplement the "assistant" functions currently provided by smartphones by providing additional senses and outputs, whether the computer using them is worn or driven.

Today, smartphone applications remind you of where you parked.[21] Some proactively prompt you and point out nearby restaurants and convenience stores.[22] They access your calendar and suggest routes to your next appointment.[23] Such applications are able to use even more specific data: the time of day and a history of restaurants you've parked at, to identify you as a likely customer and present you with a customized prospect of visiting a restaurant you're approaching. App manufacturers will sell this service to restaurants, and the ones that pay will be preferred, if not exclusively recommended.

The vehicle of the future may be equipped to sense medical data[24] non-invasively in order to tell if the driver is intoxicated, sleepy, or ill and deny control of the vehicle or call for help appropriately. Infrared cameras can sense body temperature and respiration parameters[25] such as rate, depth, and regularity, and even the driver's emotions.[26] 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 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 it if approved.[27] It will certainly be aware of the amount of remaining fuel and will point out gas or recharge stations as appropriate.[28]

20 Bill Howard, *Car Navigation Is a Ripoff. Here's Why*, EXTREMETECH, http://www.extremetech.com/extreme/96175-car-navigation-is-a-ripoff-here%e2%80%99s-why (last visited Sept. 12, 2016).

21 Jon Russell, *Google Now Adds Parking Reminder*, THE NEXT WEB, May 1, 2014, http://thenextweb.com/google/2014/05/01/google-now-gets-parking-detector-remind-left-car/.

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

23 Paul Sawyers, *Waze for Android Taps Your Calendar Events to Tell You When to Leave Based on Traffic Conditions*, VENTUREBEAT, http://venturebeat.com/2016/03/10/waze-for-android-taps-your-calendar-events-to-tell-you-when-to-leave-based-on-traffic-conditions/ (last visited Sept. 12, 2016).

24 *"The Emergency Medical Assist": A Sensor System Designed for Automobiles That Monitors the Vital Signs of the Driver*, INVENTS COMPANY, Apr. 9, 2016, https://invents.newswire.com/news/the-emergency-medical-assist-a-sensor-system-designed-for-automobiles-9901699 (last visited Sept. 12, 2016).

25 Jin Fei and Ioannis Pavlidis, Analysis of Breathing Air Flow Patterns in Thermal Imaging, in Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE, IEEE, 2006, 946–952, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4461909.

26 *FLIR Thermal Imaging Cameras Allow -Machines to Read Human Emotions*, FLIR, http://www.flir.co.uk/cs/display/?id=67117 (last visited Sept. 12, 2016).

27 Eric Ravenscraft, *Google Now Adds Gas Stations On Your Route Cards*, LIFEHACKER, http://lifehacker.com/google-now-adds-gas-stations-on-your-route-cards-1687419012 (last visited Sept. 12, 2016).

28 *Id.*

C. LONGEVITY OF AUTOMOBILES AND COMPUTERS

Consider the longevity of a smartphone[29] vs. that of a modern automobile. A 1950s car, maintained appropriately, can still operate with acceptable safety and 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 law[30] 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 weren't 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[31].

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 on-board system.[32] 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 smartphone to an automobile's speakers and provides a speakerphone microphone for telephone calls.[33]

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 Tesla[34]) 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.

Within a few years, the computer hardware behind a navigation or entertainment system is 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.

But this paradigm of old vehicles continuing to contain old computers for their entire useful lives won't 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

29 Chris Ely, *The Life Expectancy of Electronics*, https://www.cta.tech/News/Blog/Articles/2014/September/The-Life-Expectancy-of-Electronics.aspx (last visited Sept. 12, 2016).

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

31 Casey Phillips, *How Smartphones Revolutionized Society in Less than a Decade*, http://www.govtech.com/products/How-Smartphones-Revolutionized-Society-in-Less-than-a-Decade.html (last visited Sept. 12, 2016).

32 Bill Howard, *Car Navigation Is a Ripoff. Here's Why*, EXTREMETECH, http://www.extremetech.com/extreme/96175-car-navigation-is-a-ripoff-here%e2%80%99s-why (last visited Sept. 12, 2016).

33 *Roadster 3.0 Battery Upgrade*, TESLA MOTORS, http://shop.teslamotors.com/products/roadster-3-0-upgrade (last visited Sept. 12, 2016).

34 *Id.*

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.[35] Rather than 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[36] 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.[37] Pilot training and license requirements for manned and unmanned aircraft 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.

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 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 including 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.

Thus, we can have more competition in the production of autonomous driving systems, potentially reducing their prices and increasing their capability. It is likely that the producers of such 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

35 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. Tesla has offered a $29,000 battery upgrade for their *Roadster* models even though there are only about 2000 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.

36 *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*, RACKSPACE US, https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/ (last visited Sept. 12, 2016).

37 *Flight Training with A350 XWB | Airbus, a Leading Aircraft Manufacturer*, AIRBUS, http://www.airbus.com/support/training/flight/flight-training-with-a350-xwb/ (last visited Sept. 12, 2016).

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, such that the system would drop providing the autonomous function once it is past a mandatory replacement date. This would prevent the use of "junker" computers to drive autonomously past the date when they could be expected to perform with a level of safety comparable to modern units.

The addition of a capability[38] 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 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 their property. More recently, exclusion mechanisms which operate *in the interest of the manufacturer and contrary to the interest of the owner*[39] 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.[40]

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, they 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.[41] Or they can prevent retrofitting, tuning and other modifications by using proprietary communication protocol and connector interfaces.[42] Manufacturers can withhold documentation and manuals from the end-user and makers of aftermarket modifications, so that interoperation with their on-board electronics is impossible without extensive reverse-engineering.

38 *Uconnect 5.0 Upgrade to 8.4AN (2014 Cherokee) - Part Deux*, JEEP CHEROKEE FORUMS (Apr. 18, 2015), http://jeepcherokeeclub.com/385-jeepcherokeeclub-com-how-s/123826-uconnect-5-0-upgrade-8-4an-2014-cherokee-part-deux.html (last visited Sept. 12, 2016).

39 Pete Bigelow, *Automakers to Gearheads: Stop Repairing Cars*, AUTOBLOG, http://www.autoblog.com/2015/04/20/automakers-gearheads-car-repairs/ (last visited Sept. 12, 2016).

40 *Uconnect 5.0 Upgrade to 8.4AN (2014 Cherokee) - Part Deux*, JEEP CHEROKEE FORUMS (Apr. 18, 2015), http://jeepcherokeeclub.com/385-jeepcherokeeclub-com-how-s/123826-uconnect-5-0-upgrade-8-4an-2014-cherokee-part-deux.html (last visited Sept. 12, 2016).

41 *Car Audio ISO Connector Pinout Diagram*, PINOUTSGUIDE.COM (Jan. 23, 2014), http://pinoutsguide.com/CarAudio/car_audio_iso_pinout.shtml (last visited Sept. 12, 2016).

42 Niels Koch, *The Car Entertainment System*, ALTRAN GMBH & CO. KG, 2011, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.672.7232&rep=rep1&type=pdf.

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.[43] The U.S. President and others promote open government.[44] In the information technology industry, programmers fervently promote open source code licensing.[45] Calls for open borders, open markets, open standards, open platforms, open data and open robotics have become louder.[46] "Open" stands for accessible, transparent and free from restraints.

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.[47] The razors-and-blades paradigm is used, for example, in selling consumer and small-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.[48] 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 consoles[49] or platforms to which their operating systems and games can be ported.[50]

2. Manufacturing Equipment: Ingredients and Parts

Somewhat similar to the razor-and-blade 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.[51] The International Salt Company tried to require buyers of its machines to purchase its

43 Karl Popper, The Open Society and its Enemies (1945).
44 *Open Government Initiative*, www.whitehouse.gov/open (noting "[the Obama] Administration is committed to creating an unprecedented level of openness in Government.")
45 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).
46 M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 577 et seq. (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).
47 Randal C. Picker, *The Razors-and-Blades Myth(s)*, John M. Olin Program in Law and Economics Working Paper No. 532, 2010.
48 *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. Ky. 2004).
49 *See* Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. Cal. 1992).
50 *See* Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. Cal. 2000).
51 *See* United Shoe Mach. Corp. v. United States, 258 U.S. 451 (1922).

salt.[52] Kodak and Xerox have been trying to prohibit, prevent or discourage unaffiliated companies to supply parts, add-on products or repair and maintenance services.[53]

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 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.[54]

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 + 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.

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 attempted acquisition of Intuit Inc. and bundling of its Internet Explorer browser application with the Windows operating system.[55]

More recently, Apple created an "app store" for iOS phones and tablets with tremendous economic success, a relatively open model that other providers including Microsoft, Blackberry and Google are trying to emulate with more or less success.[56] 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). 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.

52 *See* Int'l Salt Co. V. United States, 332 U.S. 392 (1947).
53 Joseph P. Bauer, *Antitrust Implications of Aftermarkets*, 52 ANTITRUST BULL. 31, 34 (2007).
54 IBM Corp. v. United States, 298 U.S. 131 (1936). *See* cases discussed *infra* note 58.
55 *U.S. v. Microsoft: Timeline*, Wired (Feb. 04, 2011), www.wired.com/2002/11/u-s-v-microsoft-timeline/.
56 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.

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 upon hardware parts for close to a century. 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.[57] 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 manufacturers are already trying to create developer ecosystems similar to mobile app platforms.[58]

When we look at the car as a "multicomputer on wheels,"[59] 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.

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

57 Joseph P. Bauer, Antitrust Implications of Aftermarkets, 52 ANTITRUST BULL. 31, 34 (2007); *See, e.g.,* Pick Mfg. Co. v. Gen. Motors Corp., 80 F.2d 641 (7th Cir. 1935); Crappone, Inc. v. Subaru of N. Eng., 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); Heatransfer Corp. v. Volkswagenwerk, A.G., 553 F.2d 964 (5th Cir. 1977); Pick Mfg. Co. V. Gen. Motors Corp., 80 F.2d 641 (7th Cir. 1935), *aff'd per curiam,* 299 U.S. 3 (1936). *See also* Bob Maxfield, Inc. v. Am. Motors Corp., 637 F2d 1033 (5th Cir. 1981); Dealer Computer Servs., Inc. v. Ford Motor Co., 2006-1 Trade Cas. (CCH) f 75,212 (S.D. Tex. 2006).

58 TIBCO White Paper, The Connected Car Finding the Intersection of Opportunity and Consumer Demand, http://www.tibco.com/assets/blt55390573d5d3cc7f/wp-mashery-the-connected-car.pdf.

59 David Sedgwick, *Cars Become Computers on Wheels*, AUTOMOTIVE NEWS, April 21, 2014, www.autonews.com/article/20140421/OEM06/304219993/cars-become-computers-on-wheels.

secure even if a criminal knows every detail of its operation. Security researchers[60] 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. The 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.[61]

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.

60 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 mis-application 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.

61 Tom Espiner, Trend Micro: Open Source Is More Secure, Antivirus vendor wades into the debate over the merits of open and closed code, while Red Hat takes a cautious approach, ZDNET, www.zdnet.com/news/trend-micro-opensource-is-more-secure/148445 (2006); but see also N. Gamer, The problem with open source malware, http://blog.trendmicro.com/the-problem-with-open-source-malware/ (2016).

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 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.[62] 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.[63]

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 cyber-attacks, 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 ports 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 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

62 Derek H. Swanson & Dr. Lin Wei, *United States Automotive Products Liability Law*, https://www.mcguirewoods.com/news-resources/publications/us-automotive-products-liability.pdf.
63 *See*, BGH, 09.12.1986 VI ZR 65/86 (Honda); *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).

advantage. Car manufacturers tend to control their dealer networks quite tightly and have also been known to influence consumer tests.[64]

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,[65] the agency was alerted by a security researcher about problematic software in Volkswagen diesel cars that manipulated emission tests.[66] The independent researcher triggered a wave of investigations, media reports and regulatory action, also concerning other automakers and individual auto-suppliers.[67] Had regulators adequately appreciated the benefits of independent research into automakers' software, they should 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.[68]

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

64 *See* ADAC Admits Making Up Car Award Votes, THE LOCAL, Jan. 20, 2014, http://www.thelocal.de/20140120/adac-boss-cooks-car-award-votes.

65 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.

66 *Meet John German: The Man Who Helped Expose Volkswagen's Emissions Scandal*, THE GUARDIAN, Sept. 26, 2016, www.theguardian.com/business/2015/sep/26/volkswagen-scandal-emissions-tests-john-german-research; Russell Hotten, *Volkswagen: The Scandal Explained*, BBC, Dec. 10, 2015, http://www.bbc.com/news/business-34324772.

67 *See*, *Die Autoindustrie unter Generalverdacht* [Car Industry under General Suspicion], 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, 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 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; *Bosch 'Helped Conceal' Volkswagen's Emissions Cheating Devices*, FRANCE 24, Sept. 7, 2016, www.france24.com/en/20160907-bosch-helped-conceal-volkswagens-emissions-cheating-devices.

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

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 theoretical level and competitive market, we could let the market decide upon the degree of openness necessary, and 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,[69] and the automotive sector employed 5.6% of all EU workers in 2013.[70] 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 in the last downturn.[71] Germany invested $1.1 billion towards subsidizing electric-powered cars,[72] and many other countries have implemented various schemes to promote electric vehicle sales, including fuel, road and registration tax exemptions.[73] As such, the automotive industry shares a uniquely deep economic relationship with various national governments and consequently have to endure a lesser

69 *Contribution of the Automotive Industry to the Economies of All Fifty States and the United States*, CENTER FOR AUTOMOTIVE RESEARCH (June 2011), www.autoalliance.org/files/dmfile/2015-Auto-Industry-Jobs-Report.pdf.

70 *Employment Trends*, EUROPEAN AUTOMOBILE MANUFACTURERS ASSOCIATION, www.acea.be/statistics/tag/category/employment-trends.

71 Brent Snavely, *Final Tally: Taxpayers Auto Bailout loss $9.3B*, DETROIT FREE PRESS, Dec. 30, 2014, 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.

72 Bruce Brown, *Germany Announces $1.1 Billion in Subsidies for Electric Cars*, DIGITAL TRENDS, Apr. 28, 2016, www.digitaltrends.com/cars/germany-electric-car-subsidy/.

73Overview of Purchase and Tax Incentives for Electric Vehicles in the EU in 2016, EUROPEAN AUTOMOBILE MANUFACTURERS ASSOCIATION (Apr. 8, 2016), http://www.acea.be/uploads/publications/Electric_vehicles_overview_2016.pdf. China too has subsidized it's electric vehicle market. Christian Shepard, *China Shifts Gears to Drive Electric Car Development*, FINANCIAL TIMES, Feb. 25, 2016, http://www.ft.com/cms/s/0/a55e7d36-db8a-11e5-a72f-1e7744c66818.html.

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 anti-competitive strategies to close markets to effective competition.[74] 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 hacking into onboard 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.[75]

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,[76] tried to lock down personal computers in the interest of data and cybersecurity in an initiative broadly referred to as "trusted computing."[77] 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)

74 *See infra* Section 4.2.

75 Pete Biglow, *Feds Fretting over Remove Hack of Jeep Cherokee*, AUTOBLOG (July 23, 2016), http://www.autoblog.com/2015/07/23/feds-fretting-jeep-cherokee-remote-hack-exclusive/.

76 For a full list of members of Trusted Computing Group, *see* Trusted Computing Group - Member Companies, http://www.trustedcomputinggroup.org/about/member-companies/.

77 In 2002, Microsoft launched its Trustworthy Computing initiative (originally known as "Palladium" but now more better known as "Next-generation Secure Computing Base" ("NGSCB")). For further details, *see* (i) two Microsoft white papers about the topic (Craig Mundie et al., *Trustworthy Computing*, Microsoft White Paper (Oct. 2002), http://download.microsoft.com/documents/australia/about/trustworthy_comp.doc and Windows Platform Design Notes, *Security Model for the Next-Generation Secure Computing Base* (2003), www.microsoft.com/resources/ngscb/documents/ngscb_security_model.doc), (ii) Bill Gate's email to Microsoft employees about the initiative (reported by Wired.com and accessible at http://www.wired.com/2002/01/bill-gates-trustworthy-computing/) and (iii) general technical information about NGSCB (accessible at https://msdn.microsoft.com/en-us/library/cc723472.aspx). 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. However, detractors argued that NGSCB was in effect "Treacherous 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.

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.[78] 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, and make computers safer, more secure and reliable for end-users.[79] Critics, 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.[80] 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 e-book software word processor company may similarly be ordered by authorities to remotely delete a publication that expresses a contrary viewpoint to that of the government.[81] Further, critics argue that "trusted computing" will increase anti-competitive monopolistic behavior as users, particularly businesses, become locked into incumbent "trusted computing" platforms.

78 For an overview of the technical aspects of "trusted computing," *see generally* Ross Anderson, *Cryptography and Competition Policy - Issues with "Trusted Computing,"* CAMBRIDGE UNIVERSITY (2003), https://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf.

79 *See generally* Craig Mundie et al., *Trustworthy Computing*, Microsoft White Paper (Oct. 2002), http://download.microsoft.com/documents/australia/about/trustworthy_comp.doc; *See* Carolin Latze and Ulrich Ultes-Nitsche, *Stronger Authentication in E-Commerce: How to Protect Even Naïve User Against Phishing, Pharming and MITM Attacks* (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 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*, http://electronicdesign.com/microprocessors/understanding-trusted-computing-ground; *see also* Hans Brandl and Thomas Rosteck, *Technology, Implementation and Application of the Trusted Computing Group Standard*, Infineon White Paper (2004),
http://www.infineon.com/dgdl/Trusted+Computing+Overview.pdf?fileId=db3a304412b407950112b416592f203e;
Windows Platform Design Notes, *Security Model for the Next-Generation Secure Computing Base* (2003), www.microsoft.com/resources/ngscb/documents/ngscb_security_model.doc.

80 *See* Richard Stallman, "Can you trust your computer?", https://www.gnu.org/philosophy/can-you-trust.en.html. *See also* Benjamin Stephan's 2007 lighthearted short video questioning the merits of trusted computing that won Adobe's Design Achievement Award for Motion Graphics ("Trusted Computing" accessible at http://www.adaagallery.com/benjaminstephan/video/1/).

81 *See* Ross Anderson, *Trusted Computing Frequently Asked Questions* (2003), http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

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.[82]

The debate over the merits and dangers of "trusted computing" polarized the industry and consumers for many years, with the controversies preventing any true widespread adoption, outside of the military.[83] More recently, interest in "trusted computing" has increased again due to potential uses in cloud[84] and mobile computing.[85] 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 a dead-end road for the closed car.

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 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.[86]

82 Ross Anderson, *Cryptography and Competition Policy - Issues with "Trusted Computing,"* CAMBRIDGE UNIVERSITY (2003), Section 6.2, https://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf.

83 For a brief discussion why industry adoption of "trusted computing" has been slow, *see* "Defining and Selling Trusted Computing," 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 Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media*, Department of Defense Memorandum , 2007; William Jackson, *The Quest for the Holy Grail*, WASHINGTON TECHNOLOGY, Oct. 12, 2007, https://washingtontechnology.com/articles/2007/10/12/the-quest-for-the-holy-grail.aspx; and Donald Palmer, *Changing Military Operations Demand Fail-Safe Solutions in Cyber Security* (2012), http://www.militaryaerospace.com/articles/print/volume-23/issue-09/opinion/changing-military-operations-demand-fail-safe-solutions-in-cyber-security.html.

84 *See generally* Eghbal Ghazizadeh et al., *Trusted Computing Strengthens Cloud Authentication*, SCIENTIFIC WORLD JOURNAL, 2014, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3948200/; *see also* Pardeep Kumar et al., *Effective Ways of Secure, Private and Trusted Cloud Computing*, INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ISSUES, VOL 8 ISSUE 3(2), 2011, https://arxiv.org/ftp/arxiv/papers/1111/1111.3165.pdf.

85 *See* N. Asokan et al., *Mobile Trusted Computing* (2014), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6856168; Kathleen McGill, *Trusted Mobile Devices: Requirements for a Mobile Trusted Platform Module*, John Hopkins APL Technical Digest, Vol 32 (2), 2013, http://www.jhuapl.edu/techdigest/TD/td3202/32_02-McGill.pdf; and Bill Ray, *Trusted Computing: It's BACK, and Already in a Pocket Near You*, THE REGISTER, Feb. 29, 2012, http://www.theregister.co.uk/2012/02/29/trusted_computing/.

86 *See* Comments of General Motors LLC to U.S. Copyright Office re. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07 (Mar. 27, 2015), p. 6, www.copyright.gov/1201/2015/comments-032715/; *see also* Jim Motavalli, *The Dozens of Computers That Make Modern Cars Go (and Stop)*, THE NEW YORK TIMES, Feb. 4, 2010,

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 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 are multiple-use products that are not solely or even expressly marketed as automotive products, *e.g.*, 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 OEMs. The many recalls and historic scandals relating to automotive safety[87] highlight this particularly serious policy concern. Smaller and start-up 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.

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.[88] 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. 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.

www.nytimes.com/2010/02/05/technology/05electronics.html; Robert N. Charette, *This Car Runs on Code*, IEEE SPECTRUM, Feb. 9, 2009, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

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

88 *Meet John German: The Man Who Helped Expose Volkswagen's Emissions Scandal*, THE GUARDIAN, Sept. 26, 2016, www.theguardian.com/business/2015/sep/26/volkswagen-scandal-emissions-tests-john-german-research

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.[89] The U.S. Constitution contemplates and nearly all policymakers around the world agree that innovators should be incentivized by exclusion rights under patent, copyright, trademarks 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 their intellectual property rights. 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,[90] misuse of copyrights,[91] and control of downstream distribution after a first sale,[92] and to protect interoperability[93] and keep interfaces open.[94] 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 many:[95] Governments can use the data to monitor traffic patterns, violations of traffic rules, automobile safety, environmental sustainability and the

89 See, Jay Lyman, *SCO Claims Linux GPL Is Unconstitutional*, www.technewsworld.com/story/31975.html and Darl McBride, *Open Letter on Copyrights*, www.sco.com/copyright/.

90 *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).

91 Lasercomb Am., Inc. v. Reynolds, 911 F.2d 970 (4th Cir. N.C. 1990).

92 *See*, *e.g.*, Bobbs-Merrill Co. v. Straus, 210 U.S. 339 (U.S. 1908); Kirtsaeng v. John Wiley & Sons, Inc., 133 S. Ct. 1351 (U.S. 2013); *see also* 17 USCS § 109.

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

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

95 David Welch, Your Car's Been Studying You Closely and Everyone Wants the Data, BLOOMBERG TECHNOLOGY, July 12, 2016.

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 competitor 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.[96] 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.[97]

Car owners may or may not want information collected by their car in an accident 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 Web 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. FTC 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,[98] home routers,[99] and software platforms.[100] 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.[101] 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

96 Archibald Preuschat, *TomTom Drives Into Speed Camera Scandal*, THE WALL STREET JOURNAL, Apr. 28, 2011. http://blogs.wsj.com/tech-europe/2011/04/28/tomtom-drives-into-speed-camera-scandal/.

97 *Id.*

98 *See*, *e.g.*, *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy*, FEDERAL TRADE COMMISSION (Sept. 4, 2014), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

99 *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk*, FEDERAL TRADE COMMISSION (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

100 *Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates,* FEDERAL TRADE COMMISSION (Dec. 21, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java.

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

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.[102] 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.

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."[103]

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 non-disclosure 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 non-disclosure. The public also

102 The European Automobile Manufacturers Associations ACEA embraces in a study of April 16 on "Connectivity" that "data is the fuel of the digital economy" (p. 3) and focus on risks resulting from access to data by "third parties" (*i.e.*, companies other than the automobile manufacturers"); in a study by Pinsent Masons on "Connected and Autonomous Vehicles: The emerging legal challenges," also published in April 2016, Prof. Neville Jackson, Ricardo, writes on p. 15 about 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.

103 Department of Defense Systems Engineering, *Initiatives - Open Systems Architecture*, OFFICE OF THE DEPUTY ASSISTANT SECRETARY OF DEFENSE, http://www.acq.osd.mil/se/initiatives/init_osa.html (last visited Sept. 12, 2016).

has an interest in being informed of security flaws and bugs which effect their safety and privacy. Software source code that is disclosed but still copyright protected 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."[104] Open source software is fully disclosed in the form preferred for software 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")[105] and data ("open data")[106] 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 and 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 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.

104 Bruce Perens, *Open Sources: Voices from the Open Source Revolution*, Text.Article, *1-56592-582-3*, Mar. 29, 1999, http://www.oreilly.com/openbook/opensources/book/perens.html.
105 John R. Ackerman, *Toward Open Source Hardware*, U. DAYTON L. REV. 34 (2008): 183.
106 *What Is Open Data?*, OPEN KNOWLEDGE INTERNATIONAL, http://opendatahandbook.org/guide/en/what-is-open-data/ (last visited Sept. 12, 2016).

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.

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.[107] The NHTSA can regulate any equipment that poses a safety concern, including emerging technologies introducing potential safety risks.[108] The currently-enacted FMVSS affect a broad range of subsystems within a car, including antilock braking systems (ABS), and electronic stability control (ESC),[109] and adaptive cruise control.[110] It is important to note the FMVSS merely set minimum safety performance requirements rather than dictating *design* specifications.[111]

The United States does not recognize the UN regulations created by the World Forum for Harmonization of Vehicle Regulation.[112] Domestic and foreign manufacturers are required to register with the NHTSA, so long as they manufacture or import any equipment covered by an FMVSS.[113] When offering a product for sale, a manufacturer is further required to self-certify that the product meets all applicable FMVSS.[114] 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.[115]

---

107 *See* 49 U.S.C. § 301; 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).

108 Request for Public Comments: Safety-Related Defects and Emerging Automotive Technologies, 81 FED. REG. 18935 (Apr. 1, 2016).

109 FMVSS Standards 101, 105, 126, NHTSA, http://www.nhtsa.gov/cars/rules/import/FMVSS/; *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).

110 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?*, EXTREME TECH, June 4, 2013, 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.*

111 49 C.F.R. § 571; *see also* NHTSA, New Manufacturers Handbook (2014), http://www.nhtsa.gov/cars/rules/maninfo/Manufacturer_Information_March2014.pdf.

112 *Best Practices for Importers*, NHTSA, http://www.nhtsa.gov/about/importsafety (last visited July 13, 2016); *see also* Stephen Edelstein, *Grey Market Cars: Everything You Need to Know to Avoid Your Ride Get Crushed*, DIGITAL TRENDS (Aug. 20, 2013), 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 US, unless they are tested to be compliant with US car safety laws, or for limited non driving use (*e.g.*, car show displays).

113 *Best Practices for Importers*, NHTSA, http://www.nhtsa.gov/about/importsafety (last visited July 13, 2016).

114 49 C.F.R. § 571; *see also New Manufacturers Handbook*, NHTSA (2014), http://www.nhtsa.gov/cars/rules/maninfo/Manufacturer_Information_March2014.pdf.

115 49 C.F.R. § 573.6.

Aftermarket equipment manufacturers, sellers, dealers and importers are also subject to the prohibition against making required safety equipment inoperative and reporting safety-related defects.[116] 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.[117] It is illegal to market any aftermarket part that does not conform with an applicable FMVSS or would take a vehicle out-of-compliance with a safety standard ("make inoperative").[118]

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).[119] Both automakers and equipment manufacturers using new and emerging vehicle technologies and equipment are obligated to notify NHTSA of any safety-related defects.[120]

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.[121] 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 vehicle's critical safety systems (*i.e.*, systems encompassing critical control functions such as braking, steering, or acceleration)."[122]

116 49 U.S.C. § 30122(b).

117 *On the Road: U.S. Automotive Parts Industry Annual Assessment*, U.S. DEPT. OF COMMERCE (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.").

118 *See* 49 U.S.C. § 301.02; 49 C.F.R. § 571; *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.

119 *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.

120 *See* 49 C.F.R. § 573.

121 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).

122 81 Fed. Reg. 18935, 18938.

The NHTSA also considers how certain features and technologies affect driver behavior. In 2013, the agency published non-binding 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.[123]

States are free to enact further equipment regulations which adopt NHTSA's standards and their own regulations in the absence of a federal standard.[124] 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.[125] 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.[126]

States have also started to address liability concerns and the degree of openness for automotive designs in legislation.[127] 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."[128] This could effectively reduce automakers' liability concerns associated with further opening up their systems to third-party developers.[129] 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.[130] A third proposal, would amend the criminal code for computer crime involving automobiles, setting the sentence to life in prison.[131] 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

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

124 *Id.*; *see*, *e.g.*, CALIFORNIA AIR RESOURCES BOARD, http://www.arb.ca.gov/homepage.htm (last visited July 12, 2016).

125 *NHTSA Statement of Policy on Automated Vehicles*, NHTSA, http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (last visited July 12, 2016). 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), http://www.digitaltrends.com/cars/nhtsa-autonomous-vehicle-guidelines/.

126 *Autonomous/Self-Driving Vehicle Legislation*, NAT'L. CONF. OF STATE LEGISLATURES (July 1, 2016), http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx.

127 *Id.*

128 S.B. 997, 98th Leg., Reg. Sess. (Mi. 2016), http://www.legislature.mi.gov/(S(e3kyj5rcy0zfcuv0niutsaxw))/mileg.aspx?page=GetObject&objectname=2016-SB-0997.

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

130 S.B. 927, 98th Leg., Reg. Sess. (Mi. 2016), http://www.legislature.mi.gov/(S(dade5dsv23j3nis4gwm2rnmd))/mileg.aspx?page=GetObject&objectname=2016-SB-0927.

131 S.B. 928, 98th Leg., Reg. Sess. (Mi. 2016), http://www.legislature.mi.gov/(S(dade5dsv23j3nis4gwm2rnmd))/mileg.aspx?page=GetObject&objectname=2016-SB-0928.

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.[132]

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 (ODB-II) port, which currently serves as an easy assess 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.[133] 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 owners to possible issues.[134] 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,[135] 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.[136]

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 U.S. beginning in the same year.[137] 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.[138]

132 For more information on DMCA exemptions, *see* Maria Scheid, *New DMCA Exemptions*, THE OHIO STATE UNIVERSITY (Dec. 30, 2015).

133 *See History of the Air District*, BAY AREA AIR QUALITY MANAGEMENT DISTRICT, http://www.baaqmd.gov/about-the-air-district/history-of-air-district (last visited Sept. 1, 2016).

134 *On-Board Diagnostic II (OBD II) Systems - Fact Sheet / FAQs*, CALIFORNIA AIR RESOURCES BOARD (last updated Oct. 28, 2015), https://www.arb.ca.gov/msprog/obdprog/obdfaq.htm.

135 *Id.*

136 *On-Board Diagnostics (OBD) Program*, CALIFORNIA AIR RESOURCES BOARD, http://www.arb.ca.gov/msprog/obdprog/obdprog.htm (last visited Mar. 21, 2016).

137 *On-Board Diagnostic II (OBD II) Systems - Fact Sheet / FAQs*, CALIFORNIA AIR RESOURCES BOARD (last updated Oct. 28, 2015), https://www.arb.ca.gov/msprog/obdprog/obdfaq.htm.

138 *Environmental Fact Sheet*, EPA (May 1997), https://www3.epa.gov/otaq/consumer/obd-faq.pdf. Computer-based early warning system are required by the 1990 CAA and comes standard on all MY1996 and newer light-duty cars and trucks.

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.[139] 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.[140] While it is currently permitted for an ECU to be replaced in the aftermarket, the part must comply with standards including the OBD-II protocol, or the owner and mechanic could be subject to penalties.[141]

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 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.[142]

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)[143] 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 at the cost of emissions-law compliance. Tuners use hardware interfaces such as the OpenPort 2.0[144] to access the ECU

139 *See EPA Emission Standards Reference Guide for On-road and Nonroad Vehicles and Engines*, EPA (last visited July 12, 2016), https://www.epa.gov/emission-standards-reference-guide.

140 *On-Board Diagnostics (OBD) Program*, CALIFORNIA AIR RESOURCES BOARD, http://www.arb.ca.gov/msprog/obdprog/obdprog.htm (last visited Mar. 21, 2016).

141 *See Keeping Your Mod's Warranty Intact (for Dummies)*, http://www.dummies.com/how-to/content/keeping-your-mods-warranty-intact.html.

142 *Implementing Instructions for Executive Order 13693, Planning for Federal Sustainability in the Next Decade*, OFFICE OF FEDERAL SUSTAINABILITY (June 10, 2015), 37–38 (implementing § 3(g)(iii) of the Executive Order).

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

144 Tactrix provides a hardware implementation of this standard. *See* Tactrix Openport 2.0, TACTRIX, http://www.tactrix.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=17&category_id=6&option=com_virtuemart&Itemid=53&vmcchk=1&Itemid=53t.

through the OBD-II interface, then use software such as EcuFlash[145] 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.[146] The package is software-based, installed by authorized dealers and does not void the warranty.[147]

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.[148] Though most available applications focus on diagnostic features such as decoding "check engine" light warnings, tracking fuel efficiency and locating a parked car,[149] 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.[150] 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-touch window functions, turning daytime running lights on or off and controlling a variety of other user settings.[151]

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 (ECUs) within the modern car.[152] 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.[153] 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.[154] 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,

145 *See EcuFlash – Freedom to Tune,* TACTRIX, http://www.tactrix.com/index.php?option=com_content&view=article&id=55:image3&catid=35:iceslider.
146 *Model Overview*, POLESTAR, https://www.polestar.com/us/products/model-overview/.
147 Description of *Polestar*'s relationship with *Volvo*, POLESTAR, https://www.polestar.com/us/products/optimised/
148 See, www.bafxpro.com/obdreader/ and Dan Seifert, *Samsung's New Dongle Gives Your Car an LTE Connection*, THE VERGE, Feb. 21, 2016, www.theverge.com/2016/2/21/11081476/samsung-connected-car-lte-dongle-mwc-2016.
149 Product homepage for *Automatic*, AUTOMATIC, https://www.automatic.com/home/.
150 Product homepage for *Remote for Nissan (OBD2)*, APPLE, https://itunes.apple.com/us/app/remote-for-nissan-obd2/id821598835?mt=8.
151 Product homepage for *Carista*, CARISTA, http://www.caristaapp.com/.
152 ISO 11898-1:2015, *Road vehicles -- Controller area network (CAN)*, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63648.
153 Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway--With Me In It*, WIRED, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
154 *Id.*

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.[155] 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 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.[156] Massachusetts enacted a Right to Repair bill in 2012.[157] 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.[158] 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.[159]

155 Andy Greenberg, *Chrysler Catches Flack for Patching Hack Via Mailed USB*, WIRED, Sept. 3, 2015, https://www.wired.com/2015/09/chrysler-gets-flak-patching-hack-via-mailed-usb/.

156 Homepage for *Right to Repair Coalition*, http://www.righttorepair.org/main/default.aspx. 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.

157 *Id.*

158 Gabe Nelson, *Automakers agree to right to repair deal*, AUTO NEWS, Jan. 25, 2014, 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.

159 *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.[160] 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.[161]

Right to Repair-legislation and ensuing industry self-regulation are directly focused on protecting a basic level of openness in cars. Such laws and regulations directionally support the 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 and reserves 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 U.S. and every other territory they intend to reach.[162] They may also benefit from bands reserved for automotive-specific use.[163] Cars using commercial mobile network 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."[164]

160 Homepage for *The Coalition for Auto Repair Equality*, CARE, http://www.careauto.org/.

161 RIGHT TO REPAIR ACT, H.R. 1449, 112th Cong., 1st Sess. (2012), https://www.congress.gov/bill/112th-congress/house-bill/1449.

162 *See Table of Frequency Allocations Chart*, FCC, https://www.fcc.gov/engineering-technology/policy-and-rules-division/radio-spectrum-allocation/general/table-frequency#block-menu-block-4; *see also* 47 CFR 2.106.

163 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 U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles*, NHTSA (2014), http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles; *see also U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology*, NHTSA (2014), http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications. 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*, FCC (2016), https://www.fcc.gov/news-events/blog/2016/06/08/defining-auto-safety-life-59-ghz.

164 47 U.S.C. § 222(h)(1)(A); *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) (hereafter "Glancy"). But the FCC has historically avoided applying these regulations to vehicle communications. *See* Glancy at 679.

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, road signs, and could warn an autonomous vehicle of various hazards around it. A big problem with 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 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."[165] In effect, it limited telecommunication provider's actions when consumers unlocked their devices to access other telecommunication networks, though consumers could only do so for personal or intra-family use.[166] 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.[167] Attempts to close aftermarkets are generally suspect from an antitrust perspective, but the exact line between allowed and forbidden is not always

165 Bill Chapell, *Bill Allowing Americans To Unlock Cellphones Passes House, Heads To Obama*, NAT'L PUB. RADIO (2014), http://www.npr.org/sections/thetwo-way/2014/07/25/335351105/bill-allowing-americans-to-unlock-cellphones-passes-house-heads-to-obama.

166 *Unlocking Consumer Choice and Wireless Competition Act § 2(c)*, Pub. L. No. 144, 128 Stat. 1751 (2014), https://www.gpo.gov/fdsys/pkg/PLAW-113publ144/html/PLAW-113publ144.htm.

167 J. Thomas Rosch, *Developments in the Law of Vertical Restraints: 2012*, PRACTISING LAW INSTITUTE, 12–17, https://www.ftc.gov/sites/default/files/documents/public_statements/developments-law-vertical-restraints-2012/120507verticalrestraints.pdf

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 manufacturer (OEM).[168] 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.[169]

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).[170] 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.[171] 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.[172] 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.[173] Also, the auto industry seems receptive to open-source platforms to maintain a competitive edge, specifically with respect to

168 *On the Road: U.S. Automotive Parts Industry Assessment*, U.S. DEPT. OF COMMERCE (2011), 5–6, 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.

169 Norman W. Hawker, *Automotive Aftermarkets: A Case Study in Systems Competition*, 56 ANTITRUST BULL. 57, 59–60 (Mar. 1, 2011).

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

171 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.

172 See 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.

173 GM and other manufacturers have been integrating Apple software into their vehicles since 2014. *See GM Statement Regarding Apple CarPlay Integration*, GM (Mar. 3, 2014), http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2014/mar/0303-apple-carplay.html; *HondaLink Offers Partial Car-iPhone Integration Ahead of Apple's 'iOS in the Car' Initiative*, MACRUMERS (Jan. 23, 2014), 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/.

infotainment technology.[174] 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).[175] In 1997, Microsoft was sued for anti-competitive 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.[176] 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.[177] 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 Microsoft.[178] 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."[179] In 1999, the trial court found that Microsoft was in violation of the Sherman Antitrust Act.[180] 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.[181]

174 For more information, *see Automobile Regulation Memorandum*, specifically the "Outlook Section."

175 *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/; Walter S. Mossberg, *Microsoft Still Wins Browser Wars*, THE LEDGER, Feb. 18, 2001.

176 Carey Basala, *Antitrust Lawsuits Against Microsoft for Monopolizing Computer Software Markets*, SANS INSTITUTE (Dec. 2001), at 5, 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).

177 Rick Tetzeli with David Kirkpatrick, Competitors Cry Foul. The Justice Department Wants Its Pound of Flesh. But FORTUNE's National Polls Show: America Loves Microsoft, FORTUNE, Feb. 2, 1998, http://archive.fortune.com/magazines/fortune/fortune_archive/1998/02/02/237213/index.htm.

178 DOJ Press Release, *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..

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

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

181 Dept. of Justice, U.S. v. Microsoft Corporation Information on the Settlement (Nov. 6, 2001), https://www.justice.gov/atr/usdoj-antitrust-division-us-v-microsoft-corporation-information-settlment.

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.[182] 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.[183] Confidence in the quality of non-OEM parts appears to be growing,[184] the application of competition laws remains controversial[185] and 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.[186]

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.[187] 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."[188] 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 weary to avoid willful maintenance of market power in the aftermarkets of their products through anti-competitive means. This could take the form of restricting access to key components necessary to compete in the relevant market,[189] or the way in which an alleged

182 *See*, *e.g.*, Joseph P. Bauer, *Antitrust Implications of Aftermarkets*, 52 ANTITRUST BULL. 31, 40 (2007); *Cheap Parts Can Cost You a Bundle*, CONSUMER REPORTS, Feb. 1999, at 15, available at http://www.eddiesautobodyct.com/cheap-car-parts-can-cost-you-a-bundle/.

183 Joseph P. Bauer, *Antitrust Implications of Aftermarkets*, 52 ANTITRUST BULL. 31, 40 (2007).

184 *See On the Road: U.S. Automotive Parts Industry Annual Assessment*, U.S. DEPT. OF COMMERCE(2011), http://www.trade.gov/td/otm/assets/auto/2011Parts.pdf ("[M]any consumers no longer judge replacement/aftermarket parts on anything other than form, fit, and function, since quality parts can and do come from everywhere.").

185 *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 carsales alone but also parts and service revenue.");

186 See, e.g., 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; J. Gregory Sidak, An Antitrust Rule for Software Integration, 18 YALE J. REG 1, 2001.

187 Eastman Kodak Co. v. Image Tech. Servs., 504 U.S. 451, 481(U.S. 1992) (citing United States v. Grinnell Corp., 384 U.S. 563, 570–571 (U.S. 1966))[hereinafter "Kodak"]. 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).

188 Kodak 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.

189 *See* Kodak at 481.

monopolist integrates a software offering into its overall systems.[190] 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 plaintiff.[191] But, automakers need to remain cognizant of the possibility of monopolist claims, especially if courts begin to view cars as platforms for accepting third-party software or hardware peripherals.[192]

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.[193]

Product manufacturers are not generally required to provide any warranties to end users of their products.[194] 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.[195] Specifically, under the Magnuson-Moss Act, automakers cannot require that only branded parts be used with the product in order to retain the warranty.[196] 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.[197] To get a waiver, there must be proof that one's product won't work properly without a specified item or service.[198] Improper or incorrectly performed maintenance or repair that causes damage to original equipment may also void a warranty.[199] Although the Act covers warranties on repair or replacement parts in consumer products, warranties on services for repairs are not covered.[200]

The Clean Air Act goes even further than the Magnuson-Moss Warranty Act in two respects: First, the Clean Air Act requires that manufacturers of new motor vehicles or engines provide buyers with a written emissions warranty[201] whereas more generally, and under the Magnuson-Moss

190 United States v. Microsoft Corp., 253 F.3d 34, 58.
191 *Id.* at 59.
192 *See* Michael A. Carrier, *Unravelling the Patent-Antitrust Paradox*, 150 U.Pa. L. Rev. 761, 785 (2002) for an in-depth conversation about the cases sited in this section and their effects on antitrust doctrines.
193 *Comments of the Uniform Standards in Automotive Products Coalition*, FEDERAL TRADE COMMISSION, 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.
194 Lothar Determann & Ute Krüdewagen, *Policing Social Media*, THE RECORDER, Apr. 6, 2012
195 *Id.*; *see also* 15 U.S.C. § 2301 et seq.
196 15 U.S.C. § 2302(c). These are commonly referred to as "tie in provisions."
197 *Businessperson's Guide to Federal Warranty Law*, FTC (updated May 2015), https://www.ftc.gov/tips-advice/business-center/guidance/businesspersons-guide-federal-warranty-law.
198 *Id.*
199 *Id.*
200 *Id.*
201 *See* 42 U.S.C. § 7541; *see also Comments of the Uniform Standards in Automotive Products Coalition*, FEDERAL TRADE COMMISSION, 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.

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."[202]

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 exclusion 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 exclusion 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 similar challenges from patents as 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.[203] 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

202 *See* 42 U.S.C. § 7541; *see also Comments of the Uniform Standards in Automotive Products Coalition*, FEDERAL TRADE COMMISSION, 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.

203 *The State of Innovation in the Automotive Industry 2015*, THOMPSON REUTERS, http://ip-science.thomsonreuters.com/ip/SOI-Automotive-Industry-Report.pdf. 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.*

limitations in *Alice*[204] and U.S. Congress offered in the America Invents Act (AIA) additional options to challenge patents before the patent office.[205]

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 enforcement[206] 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."[207] Furthermore, Toyota, Hyundai, Kia and Ford have joined the Open Invention Network ("OIN"),[208] "a defensive patent pool and community of patent non-aggression" dedicated to the protection of Linux and open source software.[209] Members of OIN share their patents under an agreement that provides royalty-free, worldwide, non-exclusive, non-transferable license under OIN patents.[210] 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 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 non-discriminatory (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.[211] In fact, at least one industry SSO has adopted open-source software policies,[212] and seemingly every major auto manufacturer works with Android Auto to support an open development model for infotainment apps.[213] Furthermore, Ford and Toyota are adopting SmartDeviceLink (SDL), an open-source platform for in-vehicle software. If this spirit of openness

204 *Alice Corp. v. CLS Bank International*, 134 S. Ct. 2347 (2014); *see also* 35 U.S.C. § 101.

205 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). *Patent Trial and Appeal Board Statistics*, USPTO (May 31, 2016), https://www.uspto.gov/sites/default/files/documents/2016-5-31%20PTAB.pdf.

206 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.

207 *Id.*

208 *The OIN Community*, OPEN INNOVATION NETWORK, http://www.openinventionnetwork.com/community-of-licensees/

209 Homepage for the *Open Innovation Network*, OPEN INNOVATION NETWORK, http://www.openinventionnetwork.com/; *see also* Steven J. Vaughn-Nichols, *Toyota throws weight behind Linux patent protection group*, ZDNET (July 18, 2016), http://www.zdnet.com/article/toyota-throws-weight-behind-linux-patent-protection-group/.

210 *OIN License Agreement*, OPEN INNOVATION NETWORK, http://www.openinventionnetwork.com/joining-oin/oin-license-agreement/.

211 *See*, *e.g.*, CAR CONNECTIVITY CONSORTIUM, http://carconnectivity.org/; *see also* CONSUMER ELECTRONICS FOR AUTOMOTIVE, https://ce4a.de/.

212 GENIVI, https://www.genivi.org/.

213 *Introducing the Open Automotive Alliance*, OPEN AUTO ALLIANCE, http://www.openautoalliance.net/; Product homepage for *Android Auto*, GOOGLE, https://www.android.com/auto/.

and interoperability persists, automakers may render RAND cross-licensing agreements for software patents moot.

2. Design Patents

Besides utility patents, automobile manufacturers have found design-patent protection very attractive.[214] The number of automobile parts protected by design patents has increased dramatically in recent years.[215] From 2009 to 2014, the PTO issued over 1,700 design patents to the top five automakers alone.[216] Design patent owners can enforce their patents in proceedings before the U.S. International Trade Commission (ITC) to block the importation of infringing parts[217] and sell OEM parts at higher prices.[218]

Aftermarket parts makers and insurance companies have pushed legislation to reduce the period car companies can enforce design patents.[219] The PARTS Act was introduced in 2015 to Congress.[220] The bill would reduce the period during which car companies can enforce design patents on collision repair parts from 14 years to 30 months.[221] Some of the benefits proponents point to include: (1) keeping costs down for consumers;[222] (2) preserving competition; and, (3) bringing U.S.

214 In order to obtain a design patent, a the U.S. Patent and Trademark Office (PTO) 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 U.S. recognizes 35 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, *i.e.*, not the result of, its functionality. *See Comments To The U. S. Patent And Trademark Office On Pending Legislation H. R. 5638*, USPTO (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*, AAI (Mar. 22, 2010), http://www.antitrustinstitute.org/sites/default/files/aai%20collision%20repair%20parts%20commentary_032220101350.pdf.

215 *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/.

216 In 2014 the five top automakers were GM, Ford, Toyota, Fiat and Honda. *Top 10 automakers by US Sales 2014* (Jan. 5, 2015), washingtontimes.com/news/2015/jan/5/top-10/automakers-by-us-sales-in-2014/

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

218 Remarks of Jack Gillis, Director of Public Affairs, Consumer Federation of America (June 16, 2008), http://www.uspto.gov/sites/default/files/web/offices/pac/dapp/opla/comments/designstownhall/consumerfederationamerica.pdf.

219 *See*, *e.g.*, PARTS Act, H.R. 1057 and S. 560, 114th Cong. (2015); Access to Repair Act, H.R. 3059, 111th Cong. (2009). Senator Whitehouse of Rhode Island introduced essentially the same bill in the Senate. S. 1368, 111th Cong. (2009)(No vote).

220 PARTS Act, H.R. 1057 and S. 560 (Feb. 2015)

221 PARTS Act, H.R. 1057 and S. 560 (Feb. 2015).

222 *See* Frederick R. Warren-Boulton, Economist, MiCRA, Comments for the U.S. Patent & Trademark Office Town Hall Meeting on the Protection of Industrial Designs 2 (June 16,2008), http://www.qualitypartscoalition.com/pdfs/072407/MiCRA.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.").

in line with EU and Australian law.[223] 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 U.S. to create vehicles that appeal specifically to American consumers.[224] 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 criticized design patents and some have even called for the total elimination of design patents.[225]

3. Copyright Law

Companies have to design aftermarket parts and products with functionality and interfaces that are compatible with software and electronic control units (ECUs) 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.[226] 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.[227]

b) Resale and Essential Step Doctrine

Under Section 117 of the U.S. Copyright Act, lawful owners of software copies sold pre-installed 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 customers and end users never become

223 *See Support for PARTS Act (2015)*, QUALITY PARTS COALITION, http://www.keepautopartsaffordable.org; *see also* Norman W. Hawker, *Automotive Aftermarkets: A Case Study in Systems Competition*, 56 ANTITRUST BULL. 57 (2011).

224 *See*, *e.g.*, Written Statement by Kelly Burris, COMMITTEE ON THE JUDICIARY (Feb. 2, 2015); 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 "At 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.* Quality Parts Coalition Letter to Committee on the Judiciary (Apr. 21, 2015).

225 Norman W. Hawker, *Automotive Aftermarkets: A Case Study in Systems Competition*, 56 ANTITRUST BULL. 57 (2011); 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); Annette Kur, *Limiting IP Protection for Competition Policy Reasons-A Case Study Based on the EU Spare-Parts-Design Discussion,* RES. HANDBOOK ON INTELL. PROP. L. & COMPETITION L. 313, 327 (Josef Drexl ed., 2008). No law review articles "in defense" of design patents were found.

226 17 U.S.C. §102.

227 *See* Oracle Am., Inc. v. Google Inc., 750 F.3d 1339 (Fed. Cir. 2014), *enforced* 2016 U.S. Dist. LEXIS 39675 (N.D. Cal. Mar. 25, 2016); *see also Lexmark*, *supra*; *Chamberlain*, *supra*; *Sega*, *supra* note; *Sony*, *supra* note.

"owners" entitled under Sections 109 (first sale doctrine) or 117 (limited protection for computer programs) of the U.S. Copyright Act.[228] Car manufacturers have reserved the possibility to take similar positions.[229] 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.[230] 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.[231]

c) Open Source Code Licenses

The automotive industry has increasingly been using open source software, particularly for navigation and entertainment systems.[232] 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.[233]

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

228 *See* Vernor v. Autodesk, Inc., 621 F.3d 1102 (9th Cir. 2010); *see also Contracts, Copyright, and Confusion: Revisiting the Enforceability of "Shrinkwrap,"* 5 CHI.-KENT J. INTELL. PROP. 12 (2005)

229 *See*, Comments of General Motors LLC to U.S. Copyright Office re. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07 (Mar. 27, 2015), p. 12, www.copyright.gov/1201/2015/comments-032715/.

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

231 Kirtsaeng v. John Wiley & Sons, Inc., 133 S. Ct. 1351, 1389 (U.S. 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.").

232 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/

233 Under Section 6 of GPLv3, 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 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 FOUNDATION (June 2007), https://www.gnu.org/licenses/gpl-3.0.en.html; Jeremiah Foster, *Driven to Tears -- GPLv3 and the Automotive Industry*, INT'L FREE & OPEN SOURCE SOFTWARE L. REV. (Jan. 7 2016), http://www.ifosslr.org/ifosslr/article/view/102; Jonathan Corbet, *LFCS: GPLv3 and Automobiles*, LWN.NET, https://lwn.net/Articles/548212/.

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 Sections 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.[234]

The Copyright offices excluded from said exemption 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.[235] With this exclusion, the Copyright office seeks to protect copyright owner interests in entertainment content and maps but not preclude, for example, makers of aftermarket entertainment or telematics systems to access other ECUs or create their own ECUs to substitute original entertainment or telematics products or establish connectivity between their products and existing cars.

4. Computer Interference Laws

The Computer Fraud and Abuse Act (CFAA) and other computer interference laws[236] prohibit and sanction circumvention of technical protection measures. According to the CFAA, one may not access a computer without or exceeding authorization to obtain information.[237] 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.

234 See Library of Congress, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 80 FR 65944 (Oct. 28, 2015), https://federalregister.gov/a/2015-27212.

235 *Id.* at 65954.

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

237 18 U.S.C. § 1030 (a)(1).

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.[238] Facebook has similarly been successful in using the Computer Fraud and Abuse Act as a tool against other companies scraping its data.[239] 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.[240] 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,"[241] 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."[242] Automobile manufacturers cannot use trademark law to prevent aftermarket part suppliers from referring to original part numbers[243] or using comparative advertising to show their aftermarket products or parts are compatible with—or improvements over—the originals.[244] Similarly, automobile manufacturers

238 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, http://arstechnica.com/tech-policy/2015/06/3taps-to-pay-craigslist-1-million-to-end-lengthy-lawsuit-will-shut-down/.

239 Facebook, Inc. v. Power Ventures, Inc., 2016 U.S. App. LEXIS 12781 (9th Cir. 2016).

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

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

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

243 *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, 2012 U.S. Dist. LEXIS 155599 (C.D. Cal. 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. Appx. 841, 846 (6th Cir. 2010) (holding that plaintiff did not meet their burden with respect to part numbers).

244 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

cannot assert their trademarks to prevent third party repair shops from advertising their proficiencies in supporting particular vehicle models.[245]

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 and 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.[246] 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.[247]

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 data."[248] 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,[249] 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 U.S. that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to

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*, INTA BULLETIN (2012), http://www.inta.org/INTABulletin/Pages/NotAllIsFair(Use)inTrademarksandCopyrights.aspx.

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

246 *See* Kewanee v. Bicron, 416 U.S. 470, 475 (U.S. 1974) ("trade secret law . . . does not offer protection against discovery by fair and honest means, such as . . . reverse engineering"). *See also* Uniform Trade Secrets Act With 1985 Amendments § 1, cmt., NAT'L CONFERENCE OF COMM'RS OF UNIF. STATE LAWS 1985, http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf; DEFEND TRADE SECRETS ACT OF 2016, Pub. L. No. 153, 130 Stat. 376.

247 See Lothar Determann, Luisa Schmaus and Jonathan Tam, New Trade Secret Law in the EU and U.S. (forthcoming 2016).

248 Paul Schwartz, *Property, Privacy, and Personal Data* 117 Harv. L. Review, 2055, 2059 (2004).

249 *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 ("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 (

another."[250] 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),[251] which serve as black boxes to record critical sensor and diagnostic data prior to collisions.[252] 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.[253] Further, seventeen states have enacted their own statutes regulating EDR data disclosure, as of January 2016.[254]

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).[255] Given the privacy implications, automakers in the U.S.—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.[256]

The U.S. federal government is also considering creating a formal system of protection that is align with these goals, through the SPY Car Act. The associated bill was introduced to Congress in 2015 and, if enacted, would require 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 U.S.[257] 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.[258] The proposed legislation would also impose penalties of up to $1 million on automakers that fail to file a privacy policy or

250 United States v. Knotts, 460 U.S. 276, 281 (U.S. 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.").

251 Martin Kaste, *Yes, Your New Car Has A "Black Box." Where's The Off Switch?*, NPR (Mar. 20, 2013), http://www.npr.org/sections/alltechconsidered/2013/03/20/174827589/yes-your-new-car-has-a-black-box-wheres-the-off-switch.

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

253 Fixing America's Surface Transportation Act §§ 24301–35, Pub. L. No. 114-94, 129 Stat. 1312.

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

255 *See supra* Section 4.1.2.

256 *See Privacy Principles for Vehicle Technologies and Services*, AUTO ALLIANCE, http://www.autoalliance.org/auto-issues/automotive-privacy/principles.

257 SPY CAR ACT OF 2015, S.106, 114th Cong., 1st Sess. (2015–2016), https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info. 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.

258 Hearing entitled "Examining Ways to Improve Vehicle and Roadway Safety" (Oct. 2015), http://docs.house.gov/meetings/IF/IF17/20151021/104070/HHRG-114-IF17-20151021-SD002.pdf.

comply with an express privacy policy and fines of up to $100,000 for failing to prevent computer crime.[259] The proposed legislation would also require the NHTSA to create an Automotive Cybersecurity Advisory Council to develop cybersecurity best practices for vehicle manufacturers.[260]

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.[261] The term "personal data" is defined broadly as "any information relating to an identified or identifiable natural person,"[262] 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 "any 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction,"[263] which 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,[264] 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.[265] 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.[266]

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, 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.[267] Also, even if car manufacturers pursue proprietary, closed design and business models, they will likely pursue data commercialization plans,

259 *Id.*
260 *Id.*
261 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].
262 *Id.* art. 4.
263 *Id.*
264 GDPR. art. 6(1)(a).
265 *Id.* art. 7(3).
266 *Id.* Art. 6(1)(f).
267 See, Lothar Determann, California Privacy Law, 2nd Ed., Chapter 6-3:2 (2017 - forthcoming).

alone or with partners,[268] 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,[269] perhaps due to oversimplified privacy advocacy[270] and proposals for property law regimes to protect privacy.[271] 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.[272]

Companies that invest significant time and efforts into the creation of databases can claim limited protection under European database laws[273] and U.S. state laws on appropriation.[274] 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 on-board 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, *e.g.*, map data generated via navigation systems, truck fleet management pattern data compiled via telematics services or driver behavior information collected via driver assistance systems. Also, even without investing into the creation of a protectable database, companies can claim trade secret

268 See the study by the European Automobile Manufacturers Associations (ACEA) of April 2016 on "Connectivity."

269 *Cf.* Paula 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).

270 *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 COMMISSION, *How Will the Data Protection Reform Affect Social Networks?* (2012), http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf (last visited Mar. 25, 2012).

271 *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 (Spring 2002).

272 *See*, *e.g.*, 17 U.S.C. § 102(b) ("In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery . . . ."); Feist Publications, 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, cl. 8 of the U.S. Constitution for protection) (citations omitted).

273 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).

274 *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 Chicago v. Dow Jones and 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 (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 et seq. (1997).

protection for information that companies develop or acquire under confidentiality obligations and keep secret with reasonable means.[275]

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.[276] However, five state statutes broach the issue of data ownership.[277] For 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.[278] The statute closely associates this data ownership with the right to consent to retrieval and use of the collected data.[279] Oregon's corresponding statute also provides for exclusive ownership and consent rights to this data.[280] 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.[281]

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,"[282] 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.[283]

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."[284] Here, the

275 *See*, *e.g.*, CAL. CIV. CODE §3426.11.

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

277 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*, 20-11 MEALEY'S EMERG. INS. DISPS. 13 (2015).

278 ARK. CODE. § 213-112-107(c),(e) (2010).

279 *Id.*

280 ORE. REV. STAT. § 105.928

281 *See* Frederick J. Pomerantz & Aaron J. Aisen, *Auto Insurance Telematics Data Privacy And Ownership*, 20-11 MEALEY'S EMERG. INS. DISPS. 13 (2015).

282 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.").

283 *See* Kenneth Ross, *Post-Sale Duty to Warn* 9, AMERICAN BAR ASSOCIATION (2004).

284 *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

manufacturer sold a plastic molding machine that a user subsequently modified so as to compromise a safety mechanism.[285] 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."[286] 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.[287] In an analogous context of self-driving vehicles, critics are similarly weary of placing too much liability on manufacturers, or else risk innovation being stifled.[288]

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.[289] If car manufacturers are held responsible for defects caused 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

modification by the manufacturer, would place an intolerable burden on the 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).

285 *Robinson*, 49 N.Y.2d at 476–77.

286 *Id.* at 480–81.

287 *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").

288 Adam Thierer and Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars* 26, Mercatus Working Paper, MERCATUS CENTER AT GEORGE MASON UNIVERSITY (Sept. 2014), http://mercatus.org/publication/removing-roadblocks-intelligent-vehicles-and-driverless-cars.

289 *See Cox v. General 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 Equipment 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."); PRODUCT LIABILITY (LJP) § 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*, FEDERAL TRADE COMMISSION (May 2015), https://www.consumer.ftc.gov/articles/0138-auto-warranties-routine-maintenance.

throttled freedom of information on the Internet.[290] Congress also enacted special liability privileges for manufacturers of general aviation planes and firearms and similar privileges have been demanded for open robotics.[291] Some states have already enacted statutes specifically to preclude manufacturer liability for harm resulting from certain modifications such as self-driving conversion kits,[292] but the open car is not yet shielded on all roads in the United States.

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.[293]

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.

290 *See*, 230 CDA, 512 DMCA; 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); Lothar Determann, Kommunikationsfreiheit im Internet [Freedom of Communications on the Internet], p. 589 et seq. (1999).

291 *See* M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 603; see also M. Ryan Calo, *Robotics in American Law*, University of Washington School of Law Research Paper No. 2016-04 (2016). The General Aviation Revitalization Act is still in force. *See* Sikkelee v. Precision Airmotive Corp., 822 F.3d 680 (2016); www.gama.aero/advocacy/issues/product-liability/general-aviation-revitalization-act. 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 at https://en.wikipedia.org/wiki/Open-source_robotics.

292*See* Francoise Gilbert and 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. (Nv. 2013).

293 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.

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.

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.[294] Sector-specific legislation and regulation may be required if courts take a wrong turn in this respect.[295] 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.

294 *See ACEA Strategy Paper on Connectivity* 6, Eur. Automobile Mfrs. Ass'n (Apr. 2016) ("Vehicle manufacturers are unable to accept automatic (incalculable) liability for applications developed by third parties.").
295 *See supra* Section 4.5. *cf.* M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 601 (noting that the uncertain state of legal liability presents a similar hurdle for making more "open" robots).