Harvard Journal of Law & Technology
Volume 32, Number 1 Fall 2018

WHO OWNS THE DATA GENERATED BY YOUR SMART CAR?

*Sylvia Zhang**

TABLE OF CONTENTS

I. INTRODUCTION

Vehicles with autonomous capabilities could offer society convenience and mobility at an unrivaled scale.[1] As vehicles become more autonomous, or "smarter," they will also generate more data.[2] This data

* Sylvia Zhang is a J.D. candidate at Harvard Law School. Many thanks to Professor Chris Bavitz for advising the paper that led to this Note, and to Nikhil Lele, David O'Brien, Aida Joaquin, Ben Green, Albert Gidari, Paddy Leerssen, and Alicia Loh for their time, insight, and suggestions relating to this complex and interesting topic.

1. *See generally* Corey D. Harper et al., *Estimating Potential Increases in Travel with Autonomous Vehicles for the Non-Driving, Elderly and People with Travel-Restrictive Medical Conditions*, 72 TRANSP. RES. PART C: EMERGING TECH. 1 (2016) (estimating increased mobility for seniors and non-drivers provided by AVs); Cody Kamin & Daniel Morton, *Valuing the Convenience of Fully Autonomous Vehicles*, SINGAPORE-MIT ALLIANCE FOR RESEARCH AND TECHNOLOGY, https://higherlogicdownload.s3.amazonaws.com/AUVSI/3a47c2f1-97a8-4fb7-8a39-56cba0733145/UploadedImages/documents/pdfs/Posters/Valuing%20the%20Convenience%20of%20Fully%20Autonomous%20Vehicles.pdf [https://perma.cc/N7HH-87SJ] (estimating hours saved by availability of AVs).

2. *See, e.g.*, Mark van Rijmenam, *Self-driving Cars Will Create 2 Petabytes of Data, What Are the Big Data Opportunities for the Car Industry?*, DATAFLOQ (July 23, 2013), https://

may be utilized in many societally beneficial ways: it could help businesses construct better products,[3] insurance companies better manage risk,[4] governments design better infrastructure,[5] and individuals ease their busy schedules.[6] One estimate suggests that the value of "car data and shared mobility could add up to more than $1.5 *trillion* by 2030."[7] In other words, the creation of smart car data will increase the size of the economic pie.

Although smart car data can create value, it can also create opportunities to lose value: identity theft from data breaches, the loss of autonomy through government or corporate surveillance, or annoyance from persistent targeted advertising.[8] Many risks of smart car data are negative externalities primarily borne by smart car consumers.[9] While consumers will bear most of the costs, who will receive most of the benefits? How will society share the newly-minted value embodied in smart car data? According to the Coase Theorem, a principle conceived of by the famous

---

datafloq.com/read/self-driving-cars-create-2-petabytes-data-annually/172 [https://perma.cc/P9V5-9MCM].

3. *See, e.g.*, Evan Ackerman, *How Drive.ai Is Mastering Autonomous Driving with Deep Learning*, IEEE SPECTRUM (Mar. 10, 2017, 9:30 PM), https://spectrum.ieee.org/cars-that-think/transportation/self-driving/how-driveai-is-mastering-autonomous-driving-with-deep-learning [https://perma.cc/LU2U-M52D].

4. *See, e.g.*, Adam Tanner, *Data Monitoring Saves Some People Money on Car Insurance, But Some Will Pay More,* FORBES (Aug. 14, 2013, 4:21 PM), https://www.forbes.com/sites/adamtanner/2013/08/14/data-monitoring-saves-some-people-money-on-car-insurance-but-some-will-pay-more/#357b25a42334 [https://perma.cc/RNX6-YMSF].

5. *See, e.g.*, Sara Ashley O'Brien, *Uber Partners with Boston on Traffic Data*, CNN TECH (Jan. 13, 2015, 1:09 PM), http://money.cnn.com/2015/01/13/technology/uber-boston-traffic-data/index.html [https://perma.cc/8RKQ-796R] (stating that data from ride-sharing service could inform city about traffic planning, zoning changes, and parking developments).

6. *See, e.g.*, Kamin & Morton, *supra* note 1.

7. MCKINSEY & CO., *Car Data: Paving the Way to Value-Creating Mobility* 5 (Mar. 2016), https://www.the-digital-insurer.com/wp-content/uploads/2016/05/704-mckinsey_car_data_march_2016.pdf [https://perma.cc/2ZAD-SZNY] (emphasis added).

8. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1196 (2012).

9. Companies that collect data also face risks of data insecurity, such as corporate espionage or brand name harm due to security breaches. However, since the companies are in control of their own data security, any negative effects borne by them are internalized. For example, when security researchers infiltrated the software of model year 2014 and 2015 Jeep Cherokees and were able to control the hacked vehicles remotely, much of the backlash was borne by Chrysler, Jeep's parent company. *See* Andy Greenberg, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse*, WIRED (Aug. 1, 2016), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/ [https://perma.cc/4KYW-BUJB] ("Chrysler announced a recall for 1.4 million vehicles [after the hack] . . . . For Chrysler, the fix was embarrassing and costly."). When this type of harm is internalized by the vehicle manufacturer, the manufacturer is more likely to consider these harms when deciding how much to invest in the cybersecurity of future smart cars. *See* Hala Assal & Sonia Chiasson, *Motivations and Amotivations for Software Security*, PROCEEDINGS OF THE 4TH WORKSHOP ON SEC. INFO. WORKERS, 2018, at 2 (finding company reputation to motivate developers to improve security). The harms faced by consumers, however, are external to the manufacturing company and thus will not be so considered.

economist Ronald Coase, it depends on who has the right to control, or own, smart car data.

In his influential, Nobel Prize-winning paper, Coase theorized that when two parties bargain, the same allocation of resources will result regardless of which party was initially allocated the property right.[10] To illustrate, imagine the landlord of an apartment building whose tenants suffer from the air pollution caused by the operation of the factory next door. The landlord wants less pollution, but the factory owner wants to continue operating. If the landlord holds *the right to clean air*, the two parties could strike a deal where the factory owner pays the landlord for every unit of air pollution produced. This will cause the factory owner to internalize the cost of the pollution and she will be incentivized to decrease pollution, at least until her costs of doing so are higher than the costs of paying the landlord. In contrast, if the factory owner holds *the right to pollute*, the landlord would have to pay the factory owner to persuade her to produce less pollution. The landlord would figure out how much the air pollution is "costing" him (i.e., in decreased rent) and would offer the factory owner up to that amount in exchange for less pollution. The Coase Theorem proves that the amount of pollution produced in either situation is the same. A corollary is that the landlord benefits from the transaction when *he* was allocated the initial right to clean air, while the factory owner benefits when *she* was allocated the initial right to pollute.

Analogously, the Coase Theorem suggests that whoever holds initial property rights over smart car data will benefit from the value generated by that data. This concept is echoed by a recent McKinsey report asserting that "consumers will be the ultimate winners" regarding smart car data because consumers "own" the data about them and will be able to "leverage their personal data as currency."[11]

Often, the legal discussion surrounding data is solely about data *privacy*. In contrast, this Note will focus on data *ownership* because it directly affects who will control, and therefore *who will benefit from*, smart car data. Part II of this Note defines the scope of the analysis by introducing the key elements of a smart car and the types of data it may collect. Part III then analyzes potentially applicable legal regimes, including intellectual property law, the anti-circumvention provision of the Digital Millennium Copyright Act, current and potential statutory regimes, and

10. R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 2–8 (1960); *see also* Jodi Beggs, *Introduction to the Coase Theorem*, THOUGHTCO (Sept. 19, 2018), https://www.thoughtco.com/introduction-to-the-coase-theorem-1147386 [https://perma.cc/P7MY-DHZ9].

11. MCKINSEY & CO., *supra* note 7, at 8, 13.

consumer privacy policies and terms of use. The goal is to determine if, under current law, any one entity clearly owns smart car data.

II. DEFINING A "SMART CAR" AND ITS DATA

Because data collection by cars is not limited to autonomous vehicles ("AVs"), the scope of this Note is also not limited to AVs. Instead, the discussion will encompass any "smart car," which, for the purposes of this Note, will specifically refer to any personal vehicle[12] that has connectivity to the Internet, other devices, or surrounding vehicles or infrastructure, and is equipped with external or internal sensors and a method of recording data. Smart cars may be able to integrate across platforms and applications, perhaps becoming another interface where consumers' digital profiles can be accessed. This definition of a "smart car" is extremely broad and encompasses many existing models of cars. For example, an estimated 86 percent of new cars shipped in 2018 will be equipped with Bluetooth,[13] and an estimated 96 percent of model year 2013 cars are equipped with "black boxes,"[14] which record information about the car surrounding the time of a collision.[15] Thus, it is likely that nearly all relatively new cars can qualify as a "smart car" under the broad definition given here. In 2015, there were about 36 million cars with an

12. Smart car data from commercial or fleet vehicles would likely present a different question than that of personal vehicles, potentially because there may be fewer privacy concerns when the data is not about individuals and because the balance of bargaining power between an owner of a fleet of commercial smart vehicles and a smart car manufacturer would be different from that between an individual consumer and a smart car manufacturer.

13. BLUETOOTH, *Automotive*, https://www.bluetooth.com/markets/automotive [https://perma.cc/24PF-HGSX].

With Bluetooth capability, a vehicle would only implicate data collection and privacy issues if the user actively sets up a Bluetooth connection to another device that has an Internet connection and connects the vehicle to applications that authorize the collection of data and assist in transferring it to a third party. However, since Bluetooth could facilitate many types of applications or services, including hands-free calling, GPS directions, streaming music, vehicle diagnostics and maintenance, remote keys or keyless systems, and more, *see id.*, its use could still implicate a host of data ownership issues.

14. *Black Box 101: Understanding Event Data Recorders*, CONSUMER REPS. (Jan. 2014), https://www.consumerreports.org/cro/2012/10/black-box-101-understanding-event-data-recorders/index.htm [https://perma.cc/Q52H-NF9D]. Black boxes, also known as event data recorders ("EDRs"), are generally programmed to record data only for a few seconds surrounding a crash and may be triggered by sudden swerves or sharp braking. EDRs are required to collect fifteen specific points of data that would be relevant to a crash and passenger injuries, including crash force, vehicle speed, accelerator position, brake application, steering wheel angle, seatbelt engagement, airbag deployment, and occupant size. *Id.*

15. *U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety*, U.S. DEP'T. TRANSP., https://www.transportation.gov/briefing-room/us-dot-proposes-broader-use-event-data-recorders-help-improve-vehicle-safety [https://perma.cc/CS8Y-YJVS].

Internet connection on the road.[16] One study forecasts that that number will grow to 381 million by 2020 and Internet-connected cars will generate a revenue of $8.1 trillion between 2015 and 2020.[17] Smart cars are already here today *en masse*, and they will only increase in number. The undeniable emergence of smart cars emphasizes the mounting need to understand the applicable law of data ownership and to develop a proper legal regime.

Smart cars will generate and record many types of data. Table 1 presents a simplified way to organize the types of smart car data, their characteristics, and their potential uses.

Table 1: Types of Smart Car Data

Type of Data	Examples	Generated By…	Unique to Smart Cars?	Potential Valuable Uses
Identity Information	Name, gender, age, insurance information	User	No	Targeted marketing, profile-building
App Data	Usage pattern of apps (e.g., music streamed, websites visited)	User	No	In-car entertainment ("Infotainment")
Locational Data	GPS coordinates, mileage, routes taken, time spent at locations	User & Vehicle	No	Improving public transportation, traffic, or urban planning
External Sensor Data	Images captured by autonomous vehicle cameras, lidar, radar, ultrasonic readings	Vehicle	Yes	Improving machine learning, accident reconstruction
Diagnostic Data	Engine performance, tire pressure level	Vehicle	Yes	Car maintenance, optimizing manufacturer supply chain
Driving Behavior Data	Speed, acceleration, use of autonomous functions, weight of passengers	User & Vehicle	Yes	Risk management, determining insurance rates

16. Andrew Meola, *Automotive Industry Trends: IoT Connected Smart Cars & Vehicles*, BUS. INSIDER (Dec. 20, 2016, 12:12 PM), http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10 [https://perma.cc/H8TZ-MXGM].

17. *Id.*

Alone, most smart car data is not necessarily sensitive. However, smart car data may become sensitive because modern data science is often able to infer sensitive information from non-sensitive information.[18] For example, mega-retailer Target was able to predict whether a customer was pregnant, including which trimester, based only on her purchase history.[19] With the amount of information that smart cars are able to collect about the user's physical behavior (e.g., location data, driving behavior data), the user's digital behavior (e.g., application data), and the outside world (e.g., sensor data), modern data science will likely be able to infer a lot of information, much of it sensitive, about a smart car user. Because smart car data collection is usually imperceptible and constant,[20] this increases the risk that more information about smart car users will be collected than they would like. For example, if location or sensor data shows that a smart car is frequently navigating to a drug treatment clinic, the data could be used to infer that the user is seeking drug treatment, which is more likely to be sensitive information.

Sometimes, the privacy impact of "inferred" information can be mitigated if data is anonymized, but true anonymization is not always achieved.[21] For example, one study was able to re-identify people based on a correlation of anonymous Netflix movie ratings and public IMDB movie ratings, which revealed their entire Netflix histories.[22] Location data may be especially sensitive in this respect because of the uniqueness of an individual's location. A study published in *Science* showed that by utilizing just four data points of anonymized spatiotemporal points (i.e., a person's location at a given time), an anonymized database of credit card transactions could be used to uniquely re-identify 90 percent of the 1.1 million individuals in the database.[23] Moreover, knowing the price of a transaction increased the likelihood that someone could be re-identified

18. *See, e.g.*, Mohammad Malekzadeh, Richard G. Clegg, Andrea Cavallaro & Hamed Haddadi, *Protecting Sensory Data against Sensitive Inferences*, PROCEEDINGS OF THE 1ST WORKSHOP ON PRIVACY BY DESIGN IN DISTRIBUTED SYS., 2018, at 1; Anthony Quattrone et al., *Is This You? Identifying a Mobile User Using Only Diagnostic Features*, PROCEEDINGS OF THE 13TH INT'L CONFERENCE ON MOBILE AND UBIQUITOUS MULTIMEDIA, 2014, at 1; *see also*, Sheri B. Pan, Note, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 HARV. J.L. & TECH. 239, 247 (2016).

19. Pan, *supra* note 18 at 246.

20. *See id.* at 245.

21. Pete Warden, *Why You Can't Really Anonymize Your Data*, O'REILLY MEDIA (May 17, 2011), https://www.oreilly.com/ideas/anonymize-data-limits [https://perma.cc/2PRW-G3SD].

22. Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize) (Feb. 5, 2008), https://arxiv.org/pdf/cs/0610105.pdf [https://perma.cc/5G34-GKSJ].

23. Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE 536, 536 (2015).

by 22 percent.[24] Knowing just a few data points about someone's location and behavior can completely unravel anonymization.

There is a growing ability in modern data analysis to infer sensitive information from innocuous data, even from anonymous data. Although this characteristic of data may increase privacy risks to users of smart cars, it simultaneously adds value to smart car data. As discussed in Part I, that value will be captured by whichever entity is endowed with the initial ownership of the data, bringing us to the primary inquiry of this Note.

III. APPLICABLE LEGAL REGIMES

Raw data cannot be "owned" in the same legal sense that traditional intellectual property can be owned, so throughout this Note "ownership" of data will be used as a shorthand way to describe the rights or ability to access, assign, transfer, use, destroy, or exclude others from that data. This section will first discuss why data does not fall into any of the familiar intellectual property regimes. Then, this section will analyze some potential legal structures that could affect the property-like rights surrounding smart car data, including the anti-circumvention provision under U.S. copyright law, industry-specific regulations, and the contracts and privacy policies negotiated by the stakeholders themselves. Moreover, this section will analyze the problems or gaps that these structures may create.

A. Intellectual Property Law

Existing intellectual property regimes such as patent, trademark, and copyright do not apply well to the ownership of data. Patent law does not apply because data does not fall into the category of a "process, machine, manufacture, or composition of matter, or any new and useful improvement thereof."[25] Raw smart car data would not be approved as a trademark as it is not a "word, name, symbol, or device, or any combination thereof [used] to . . . distinguish goods . . . from those manufactured or sold by others and to indicate the source of the goods."[26] Lastly, copyright law does not apply because raw data are uncopyrightable facts.[27] Copyright law might create a property interest in a "compilation of facts

24. *Id.*
25. 35 U.S.C. § 101 (1952).
26. 15 U.S.C. § 1127 (2018).
27. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 351 (1991) ("In no event may copyright extend to the facts themselves.").

if the compilation represents original authorship,"[28] but the U.S. Copyright Office states that "copyright protection is not available for . . . the selection and ordering of data in a database where the collection and arrangement of the material is *a mechanical task only*, and represents no original authorship; e.g., merely transferring data from hard copy to computer storage."[29] Thus, smart car data probably does not fit within any established American property or intellectual property regime.[30]

Even without an established intellectual property regime, courts may still find that an entity has a para-property interest in smart car data if that entity has the ability to prevent others from gathering, using, or destroying the data. This is generally how trade secrets are enforced.[31] Because "the right to exclude others is generally one of the most essential sticks" in our Anglo-American understanding of a "bundle" of property rights, trade secrets can be legally protected if the secret-holder has excluded others from knowing the secret, but that protection is lost if the secret has been disclosed to others.[32] Imagine if smart car data was stored only in the physical hard drive installed in the smart car. Then, because a smart car owner would have the right to exclude others from accessing the smart car itself, the smart car owner could control what other parties have access to the data, when, and for what reasons, and thus might have enforceable para-property rights over the data in that hard drive. Although trade secret case law may not carry over to the smart car data collected about an individual, it suggests that *control* over the access to and use of smart car data may be seen by courts as a proxy for "ownership."

B. Para-Copyright Law: Software Barriers and Anti-Circumvention

Parties could potentially secure "ownership" over smart car data by controlling access to the data through software barriers. Most smart car data will be collected, stored, and transmitted by proprietary software,

---

28. U.S. COPYRIGHT OFFICE, CIRCULAR 65, COPYRIGHT REGISTRATION FOR AUTOMATED DATABASES 1 (June 2002).

29. *Id.* (emphasis added).

30. The European Union, however, has a sui generis protection scheme for databases, which is intended to harmonize and strengthen the protection afforded to databases under copyright law. Article 1(2) of the Directive defines "database" as "a collection of . . . data . . . arranged in a systematic or methodical way and individually accessible by electronic or other means." Directive 96/9/EC, European Parliament and of the Council (March 11, 1996).

31. *See* 1 ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS §§ 1.03, 1.07A (2018) (stating that information that is secret and has independent economic value may be protected as trade secrets).

32. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1011 (1984) (internal quotations removed); *see also* MILGRIM & BENSEN, *supra* note 31, at § 1.05 ("Upon information's becoming publicly disclosed or readily available it prospectively losses its character as a trade secret.").

which is protected by copyright law. Specifically, the Digital Millennium Copyright Act ("DMCA") includes an anti-circumvention provision which mandates that "no person shall circumvent a technological measure that effectively controls access to a work protected under this title" without authorization.[33] The "work protected" is the proprietary vehicle software, and operating it in an unauthorized manner, by accessing the data without permission of the software, for example, would be considered "circumvention."

Most smart car data will likely be enveloped by proprietary software owned by the vehicle manufacturer, so access to smart car data by consumers could be impeded by the DMCA anti-circumvention provision. Individual owners of smart cars likely have no ownership rights to the proprietary software that runs on their smart car;[34] instead, most smart car owners are licensees who are granted the right to use the proprietary smart car software, and the terms of use for smart cars will most likely prohibit users from tampering with or circumventing the in-vehicle technology.[35]

Such terms of use provisions might be enforceable. In a prominent Eighth Circuit case, *Davidson & Associates v. Jung*, defendants reverse engineered a computer game software to create their own version of the game.[36] The court found that, even if the reverse engineering could have been protected by fair use, "private parties are free . . . to contract away a fair use defense . . . if the contract is freely negotiated," and that the defendants had contracted the defense away when they selected "I Agree" to the game's End User License Agreement ("EULA") and Terms of Use during the installation of the game.[37] The court did not seem fazed by the high likelihood that the EULA and terms were most likely "click-

33. 17 U.S.C. § 1201(a)(1)(A) (2018).

34. Lily Hay Newman, *Who Owns the Software in the Car You Bought?*, SLATE (May 22, 2015, 2:37 PM), http://www.slate.com/blogs/future_tense/2015/05/22/gm_and_john_deere_say_they_still_own_the_software_in_cars_customers_buy.html [https://perma.cc/U8UD-3PRX]; AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP 147–48 (2016) (reporting that Mercedes-Benz's terms of service say consumers do not acquire any rights in car software, including any right to use or modify the software).

35. PERZANOWSKI & SCHULTZ, *supra* note 34; *see, e.g.*, *User Terms*, ONSTAR (May 1, 2018), https://www.onstar.com/us/en/user_terms/ [https://perma.cc/H2UA-2LU5] (requiring user not to "copy, reproduce, distribute, decompile, reverse engineer, disassemble, remove, alter, circumvent, or otherwise tamper with any security technology . . . ."). *But see* Alex Cranz, *It Only Took Six Years, But Tesla is No Longer Screwing Up Basic Software Licenses*, GIZMODO (May 21, 2018, 11:00 AM), https://gizmodo.com/it-only-took-six-years-but-tesla-is-no-longer-screwing-1826191876 [https://perma.cc/82LQ-QH3H] (reporting that some of Tesla's smart car code is open-source and legally must be made available to the public).

36. 422 F.3d 630 (8th Cir. 2005).

37. *Id.* at 639.

through" agreements that almost no users read.[38] Of course, other circuits may decide differently and retain a consumer's ability to access, use, or destroy data collected by their smart cars, potentially by applying the doctrine of fair use. However, the result in *Jung* suggests that future smart car consumers could give up any right to access or use data collected about themselves in a smart car they have legally purchased just by clicking through a user agreement for which they had no opportunity or leverage to negotiate.[39]

If the anti-circumvention statute applies to smart car owners when they attempt to access the data collected by their cars, only a regulatory exemption made by the Copyright Office could save them from liability. Such an exemption can be made if "noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected" by the anti-circumvention provision.[40] In 2015, such an exemption was granted to allow patients and doctors to circumvent pacemaker software to access health information generated by the patients' pacemakers.[41] The exemption was likely granted because the use of uncopyrightable pacemaker data is not copyright infringement, there are significant health benefits in allowing a patient to immediately access her pacemaker data, and these benefits greatly outweigh the economic harm that might be borne by the copyright owner of the pacemaker software.[42] Similarly, the use of uncopyrightable smart car data would likely not be copyright infringement. However, the use of smart car data by individuals lacks the obvious health-related urgency that pacemakers present. In addition, allowing the circumvention of smart car software creates a higher risk of economic harm to the copyright owners of smart car software. Unauthorized tinkering with smart car software could raise safety concerns, since cars often rely on the software to function properly. Given recent fatal accidents in cars with autonomous driving features,[43] the

38. David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, GUARDIAN (Mar. 3, 2017, 8:38 AM), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print [https://perma.cc/B9C3-7DNQ].

39. *See infra* Part III.D (discussing enforceability of unilateral terms of use).

40. 17 U.S.C. § 1201(a)(1)(D) (2018).

41. Andy Sellars, *DMCA Exemption Granted for Med Device Research, Patient Access to Data*, HARV. L. SCH. CYBERLAW CLINIC (Oct. 27, 2015), https://clinic.cyber.harvard.edu/2015/10/27/dmca-exception-granted-for-medical-device-research-patient-access-to-data/ [https://perma.cc/W9VA-MKE2].

42. *Id.*

43. *See, e.g.*, Johana Bhuiyan, *Tesla's Latest Autopilot Crash is Just One of Many Problems It is Now Dealing With*, RECODE (Apr. 2, 2018, 3:30 PM), https://www.recode.net/2018/4/2/17183860/tesla-crash-autopilot-elon-musk [https://perma.cc/HM27-DVXL]; Bloomberg, *Arizona Halts Uber Self-Driving Tests; Supplier Says Uber Disabled Volvo Safety System Before Fatality*, L.A. TIMES (Mar. 26, 2018, 7:10 PM), http://www.latimes.com/business/la-fi-uber-pedestrian-technology-20180326-story.html [https://perma.cc/K8JB-922V].

safety of smart cars is particularly salient and could overshadow the issue of smart car data ownership. Thus, the Copyright Office may not grant an exception for smart cars like it did for pacemakers, but an exception to the anti-circumvention law would likely be necessary to preserve the rights of vehicle owners to access data generated by their cars under a *Jung* regime.

C. Statutory Law: Industry-Specific Regulation

Industry-specific regulation may provide more answers than generalized intellectual property regimes, which are not well-suited to data ownership. First, this section will discuss the current legislative landscape surrounding autonomous vehicles, where, unfortunately, the issue of data ownership is rarely addressed. Then, this section will introduce existing regulatory systems currently governing other types of data, specifically vehicle collision data collected by Event Data Recorders ("EDRs") and medical data collected by health care providers, and consider the application of these regimes to smart car data. Lastly, this section will evaluate what type of regulatory system is the most likely to arise and govern smart car data ownership.

1. Current Regulatory Landscape of AVs

The regulatory landscape surrounding autonomous vehicles ("AVs") has been developing quickly, but most of the legislative action has been focused on the early-stage testing and safety of autonomous cars, rather than data ownership and privacy issues. Moreover, smart car data can be collected without autonomous functions, so regulations that focus solely on autonomous vehicles leave a large proportion of smart cars and the data they collect unregulated.

a. Federal Law

There is currently no law at the federal level that regulates smart car data, but the SELF DRIVE Act, a federal bill that "lays out a basic federal framework for autonomous vehicles," has passed the House of Representatives.[44] The version that passed the House contains a data privacy provision that requires AV manufacturers to develop a privacy and notification policy that enables consumers to know what type of data is be-

44. Aarian Marshall, *Congress Unites (Gasp) to Spread Self-Driving Cars Across America*, WIRED (Sept. 6, 2017, 4:33 PM), https://www.wired.com/story/congress-self-driving-car-law-bill/ [https://perma.cc/4PYQ-FU7H].

ing collected and for what purpose.[45] Mandatory consumer notification of such practices could encourage manufacturers to manage data more responsibly and reasonably, but the SELF DRIVE Act does not assign any property-like interests in the data to the consumer; it only provides the right to be notified. Moreover, manufacturers do not need to disclose the collection or sharing of data if that data is anonymized or encrypted.[46] As discussed, anonymized data, especially highly unique information such as location, is easily de-anonymized.[47] So, this provision of the SELF DRIVE Act does little to mitigate the negative externalities of data collection such as privacy.[48] Additionally, because the Act poses only a disclosure requirement but no restrictions on how the data can be used or shared, it seems to tacitly support the position that the manufacturers have "ownership" over smart car data.

b. State Law

Until the SELF DRIVE Act or other federal act is passed, any existing state laws will govern the industry. Twenty-two states and the District of Columbia have already passed laws which regulate self-driving vehicles, but most of these laws fail to thoroughly address consumer privacy or data ownership.[49] The few state bills that do touch on privacy or data are solely focused on collecting data and sharing them with government entities in order to analyze any safety issues that occur.[50] For example, a pending Massachusetts bill explicitly indicates that individuals participating in AV pilot projects are deemed to consent to the collection and analysis of safety-related data while they are in the vehicle, but says nothing about the collection of non-safety related data.[51]

There was, however, one outlier state bill that explicitly mentioned data ownership. In North Dakota, House Bill 1394, if passed, would have (1) legally endowed *the owners of AVs* as the owner of any data or information gathered by the autonomous vehicle, (2) prohibited manufacturers from sharing identifying information without the owner's con-

45. Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act, H.R. 3388, 115th Cong. § 12(a) (2017).

46. *Id.* at § 12(a)(4).

47. *See supra* Part II.

48. *See* Editorial, *Privacy Risk in Self-Driving Cars? Senate Has to Fix That Loophole in Federal Bill*, MERCURY NEWS (Sept. 14, 2017, 1:32 PM), https://www.mercurynews.com/2017/09/14/editorial-privacy-risk-in-self-driving-cars-senate-has-to-fix-that-loophole-in-federal-bill/ [https://perma.cc/5KQH-J8LC].

49. *See Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Aug. 27, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx [https://perma.cc/3Z7Q-WHM7].

50. *See* S. 1945, 190th Gen. Ct. (Mass. 2017); S. 2149, 218th Leg. (N.J. 2018).

51. H. 3422, 190th Gen. Ct. (Mass. 2017).

sent or a court order, and (3) allowed manufacturers to share anonymous data without the owner's consent.[52] However, this bill was unanimously rejected by the North Dakota Senate in March 2017.[53] H.B. 1394 was opposed by Global Automakers, a trade association of international auto manufacturers such as Toyota and Subaru.[54] Global Automakers claimed that the auto industry is already committed to protecting consumer privacy, pointing to an industry-wide privacy policies standard,[55] so H.B. 1394 would be "unnecessary and could lead to unanticipated outcomes."[56] The letter assumed, probably correctly, that the motivation for giving ownership rights to consumers was concern about consumer privacy.

However, data ownership conveys much more value than just heightened privacy. Ownership rights over data give consumers the ability to use their data as "currency" to "purchase" things like lower insurance premiums or car concierge services.[57] Global Automakers' claim that it is already committed to consumer *privacy* thus obscures the important question of consumer *welfare*. Moreover, the fate of H.B. 1394 portends future industry lobbying if other state or federal legislatures attempt to assign clear property rights to consumers.

2. Potential Approach: Event Data Recorders

EDRs are devices that record information about a car's actions and status for a short period of time right around a collision, collecting information like crash force, vehicle speed, and airbag deployment.[58] EDR data is regulated by both federal and state laws. The federal Driver Privacy Act of 2015 explicitly clarified that EDR data is "the *property* of the owner or lessee of the vehicle in which the [device] is installed," and prohibits unauthorized access (with a few exceptions, such as if the data

52. H. 1394, 65th Leg. Assemb. (N.D. 2017).

53. *Senate Passes Autonomous Vehicle Study,* BISMARCK TRIBUNE (Mar. 28, 2017), http://bismarcktribune.com/news/state-and-regional/senate-passes-autonomous-vehicle-study/article_e7ed4540-3ee4-5c77-82aa-1098503a5a46.html [https://perma.cc/7A8Q-PFBR].

54. Press Release, Global Automakers, Global Automakers Submits Automated Vehicle Testimony in North Dakota (Jan. 25, 2017), http://www.globalautomakers.org/posts/letter/global-automakers-submits-automated-vehicle-testimony-north-dakota [https://perma.cc/K6TM-URLS].

55. *See infra* Part III.D (discussing Global Automakers privacy principles in more detail).

56. Letter from Josh Fisher, Manager State Gov't Affairs, Global Automakers, to Rep. George J. Keiser, Chairman, N.D. H. Indus. Bus. & Labor Comm. (Jan. 25, 2017), http://www.globalautomakers.org/OldSiteContentAssets/letter/Global-Automakers-Submits-Automated-Vehicle-Testimony-in-North-Dakota-assets/north-dakota-hb-1394-av-data-oppose-id-12500-pdf [https://perma.cc/VYJ9-Q73H].

57. MCKINSEY & CO., *supra* note 7 at 8, 16–17.

58. Michelle V. Rafter, *Decoding What's in Your Car's Black Box*, EDMUNDS (Jul. 22, 2014), https://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html [https://perma.cc/H89R-WH7S].

is admitted to court as evidence or if it is anonymously used for traffic safety research).[59] Seventeen states have similar laws regarding EDR data: vehicle owner consent is usually required to access EDR data but there are carve-outs relating to safety, vehicle maintenance, and law enforcement.[60]

The property regime applied to EDR data is simple: vehicle owners (and lessees) own the data collected by their vehicles, with some exceptions for safety and research. If a similar regime was applied to smart car data broadly, then according to the Coase Theorem, the consumer — as opposed to the auto manufacturer industry, insurance industry, or other entities — would realize most of the value generated by smart car data. Consumers could decide to "spend" their personal data in exchange for convenience, safety, or lower insurance premiums. The exceptions that allow emergency services, courts, and transportation agencies to access the data would facilitate the actualization of benefits regarding public safety, law enforcement, and public research, benefiting society at large.

The value of EDR data is somewhat restricted by the nature of the data. EDR data is limited to a few seconds' worth of technical information, so it only provides value and insight when the vehicle has been in an accident. In contrast, smart car data likely has high potential commercial value — an estimated value of $1.5 trillion by 2030[61] — and thus industry lobbyists will have a strong incentive to fight against a consumer-friendly data ownership regime such as one that clearly gives consumers control over their data. The auto industry will fight and lobby for an interest in that data, as it did in North Dakota against H.B. 1394. Although an EDR-style regime would give consumers the ability to choose how to spend their "data currency" and facilitate the public uses of smart car data, the potential lobbying of industry interest groups makes an EDR-style regime, where consumers will receive clear ownership rights in smart car data, unlikely.

3. Potential Approach: Medical Data

Another approach of data governance can be found in the current regulatory structure of medical data. Individually identifiable health information ("medical data") is highly regulated by the federal Health In-

59. Driver Privacy Act of 2015, Pub. L. No-114-94, § 24302 (2015) (emphasis added).

60. *Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx [https://perma.cc/XL4D-WXNW].

61. MCKINSEY & CO., *supra* note 7 at 5.

surance Portability and Accountability Act ("HIPAA").[62] Data ownership is not explicitly discussed by HIPAA, but it strictly delimitates what facilities may do with protected medical data.[63] HIPAA requires health care providers and health plans ("covered entities") to give patients access to their own medical data when requested and to provide data to the Department of Health and Human Services during investigations or enforcement actions.[64] HIPAA also permits covered entities to disclose medical data without patient authorization for a litany of reasons, as represented below:

(1) Running treatment and payment operations;

(2) Informing government authorities regarding abuse, neglect, or domestic violence;

(3) Complying with government audits and investigations;

(4) Complying with court or administrative orders;

(5) Facilitating workers' compensations claims;

(6) Facilitating law enforcement (e.g., identifying a subject or victim); and

(7) Furthering research that provides generalizable knowledge.[65]

Because individuals cannot block the use of medical data about them in these contexts, they have a weak property interest in this data. Covered entities also have weak property claims to the medical data because HIPAA requires the entities to make them available to individuals and to the government, eroding the covered entities' rights to use, destroy, or prevent access to that data.

Medical data, like smart car data, is a valuable asset.[66] Analogous to smart car data, medical data can provide value to the health care industry and insurers, to law enforcement and government, to research, and to individual patients. HIPAA's strict regulatory structure addresses each of the ways that data can be valuable to society. HIPAA facilitates access to

---

62. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. 3 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/P7JR-MVGC].

63. *See* Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 72–74 (2011).

64. *Summary of the HIPAA Privacy Rule*, *supra* note 62, at 4.

65. *See id.*

66. *See, e.g.*, Mariya Yao, *Your Electronic Medical Records Could Be Worth $1000 to Hackers*, FORBES (Apr. 14, 2017, 10:05 PM), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#139ba2db50cf [https://perma.cc/2QSV-KJQY] ("On the black market . . . your social security number is [worth] 10 cents . . . . But your electronic medical health record . . . could be worth hundreds or even thousands of dollars.").

medical data to each type of entity that may have an interest in the data, preemptively distributing the potential value of medical data between them.

A HIPAA-type regulatory structure would distribute the value of smart car data to many stakeholders without explicitly defining data ownership. Within the landlord-factory example of the Coase Theorem, a HIPAA-type structure would be equivalent to the government stepping in to dictate the amount of pollution allowed, negating the need for the landlord and factory owner to negotiate. There could be benefits to such a regime applied to smart car data, such as ensuring that consumers have access to data about themselves and limiting the appropriation of the data to socially desirable uses (e.g., traffic and safety research) rather than profit-generating ones (e.g., targeted advertising). On the other hand, it cannot be guaranteed that a HIPAA-type structure would distribute smart car data in an efficient way; for example, the statutory nature of the regime means that some uses of data would be under-promoted or over-promoted, especially as technology changes.

A HIPAA-style regulatory scheme might be heavily opposed by the automobile industry. As we saw with the response to North Dakota's H.B. 1394, the auto industry is quick to respond to potential legislation that limits its property interests in smart car data.

4. Potential Approach: Bifurcation of Data

A middle ground between placating the auto industry and consumer privacy interests could be the bifurcation of smart data into "sensitive" and "non-sensitive" data and regulating them according to different standards. The SELF DRIVE Act already makes a similar distinction, requiring manufacturers to disclose their actions with data collected about vehicle occupants, but not requiring any disclosure regarding anonymized or encrypted data.[67] HIPAA also only restricts the use of health information if it is individually identifiable and relieves restrictions on the use or disclosure of data that have been properly "de-identified."[68] One possible solution for smart car data would be to assign property rights of sensitive information to the consumer, while non-sensitive information could be assigned to the auto manufacturers. If property rights to smart car data were distributed this way, the Coase Theorem suggests that auto manufacturers would be able to capture all the economic benefits from non-sensitive data, but this could theoretically be a way to address some privacy issues. Robust de-identification could also reduce the negative externalities of data sharing, such as an-

67. H.R. 3388 § 12(a), 115th Cong. (2017).
68. *Summary of the HIPAA Privacy Rule*, *supra* note 62 at 4.

noyance from targeted marketing, by making it more difficult to match up the data to an individual.

However, it will be difficult to draw a line between sensitive and non-sensitive data. Under HIPAA, medical data is considered de-identified if eighteen identifiers (including name, address, birth date, telephone number and more) are removed.[69] The same types of information could be considered sensitive for smart car data. But should location data be considered sensitive? As mentioned earlier, one study showed that 90 percent of individuals could be re-connected to their "anonymous" data by analyzing just four spatiotemporal points.[70] Similarly, images captured by a smart car's cameras could be "anonymous" but could also capture identifying images, such as images of the individual, her family, her home, or her workplace. Even other types of data that do not present obviously identifiable information, such as vehicle diagnostic information, application data, or driving behavior data, could be sensitive when multiple data sets are analyzed together and form previously unknowable connections.[71]

Lastly, statutorily or administratively categorizing data into sensitive and non-sensitive buckets would need to keep up with changing technologies. For example, if face-recognition or other image-recognition software becomes widely used, images could become much more sensitive than they are now. Sorting smart car data into "sensitive" and "non-sensitive" buckets may be quite complex and leaves room for political compromises, but could be one way for legislators to protect consumer privacy while still accommodating industry interests.

5. Debrief

In summary, as of the writing of this Note, there are currently no enacted statutes that regulate data collection in smart cars at either the state or federal level. If the SELF DRIVE Act or a similar regime regarding smart car data were to become law, consumers and public actors would be disadvantaged. Auto manufacturers would essentially "own" smart car data because they would be able to maintain complete control of the data with few restrictions on what they can do with it and to whom they can sell it. There would be no requirements for the manufacturer to share data with individuals or public actors, so individuals, governments, or researchers that want access to the data would have to bargain for it from a disadvantaged position. Think back to the landlord-factory application of the Coase Theorem. But other regimes may not be politically feasible

69. *See id.* at 19 n.15.
70. de Montjoye et al., *supra* note 23.
71. *See supra* Part II.

if the auto industry lobbies heavily. An EDR-style regime, which gives consumers ownership over the data collected by their cars, will likely be heavily opposed by the industry (as it was in North Dakota). Moreover, a heavily regulated regime like HIPAA is also unlikely as it may appear to raise the barriers to innovation, which might conflict with the stated purpose of the SELF DRIVE Act to "encourage the . . . deployment of [automated] vehicles."[72]

D. Contractual Law: Privacy Policies and Terms of Use

In the void left by a lack of statutory law, smart car data will most likely be governed through contractual law, such as privacy policies and terms of use, created by the industry itself.[73] Privacy policies are meant to inform the user about what data is collected and, in broad strokes, how and why the data is being used by the data collector or third parties.[74] Terms of use, which are also known as "terms and conditions," "terms of service," or "user agreements," allow the service provider to set the rules of use, for example by prohibiting certain user activities, limiting its own liabilities, or requiring individual arbitration.[75] Privacy policies and terms of use are almost always drafted unilaterally by the service provider, so individual users have essentially no way to negotiate their content. However, they are usually held to be enforceable when users have adequate notice and expressed assent.[76] Because of the high value of smart car data, smart car manufacturers may prefer to draft privacy policies and terms of use in a way that allows them to use and maintain control over the data, essentially becoming the de facto owners of the data. Smart car manufacturers may also want to retain the right to license or sell the data to third parties.

There are already many industries where the collection and use of valuable consumer data benefit the service provider or manufacturer. For example, internet and cellular service providers (e.g., Verizon),[77] sellers

---

72. H.R. 3388 § 2, 115th Cong. (2017).

73. *See* Raymond Millien & Christopher George, *Internet of Things: The Implications for IP Law Practice*, IPWATCHDOG (Nov. 30, 2016), https://www.ipwatchdog.com/2016/11/30/iot-implications-ip-law-practice/id=75144/ [https://perma.cc/D7ND-3HSY].

74. Sara Pegarella, *Privacy Policies vs. Terms & Conditions*, TERMSFEED (Apr. 14, 2018), https://termsfeed.com/blog/privacy-policies-vs-terms-conditions/#What8217s_a_Privacy_Policy [https://perma.cc/TZ7B-A7MQ].

75. *Id.*

76. *See* Feldman v. Google, Inc., 513 F. Supp. 2d 229, 238 (E.D. Penn. 2007); *see also* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (finding "shrinkwrap" user agreements enforceable).

77. *See Privacy Policy*, VERIZON, http://www.verizon.com/about/privacy/full-privacy-policy [https://perma.cc/RS8V-M9MA].

of hardware (e.g., Apple),[78] and platform operators (e.g., Google)[79] all generally retain the rights to use the data for their own business purposes. The vehicle industry (e.g., OnStar, an in-vehicle safety and security system)[80] has followed suit. In most cases, consumers who want to use the services of these companies have no choice but to agree to the privacy policies set by the company. OnStar's user terms state that "[y]ou are not permitted to access or use any of the Services if you do not agree to be bound by the Agreement."[81] There is no genuine ability to negotiate or to shield oneself from data collection and still use the service.[82]

Two automotive industry trade organizations, Automakers Alliance and Global Automakers, and their members, which include many major players such as Ford, GM, BMW Group, Toyota, Volvo, and more, have committed to an industry-wide set of privacy principles.[83] They have committed to principles such as "transparency," "choice," "data minimization," and "access" regarding certain user information.[84] "Transparency" means that the "collect[ion], us[age], or shar[ing] of Geolocation Information, Biometrics, or Driver Behavior Information" must be prominently disclosed to consumers.[85] "Choice" is given to consumers by requiring "affirmative consent" if those types of data are used for marketing or shared with unaffiliated third parties.[86] "Data minimization" means that automakers have committed to collecting and retaining

78. *See Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ [https://perma.cc/WY33-D256].

79. *See Privacy Policy*, GOOGLE, https://policies.google.com/privacy [https://perma.cc/8WR5-SH9H].

80. *See User Terms*, ONSTAR, https://www.onstar.com/us/en/user_terms/ [https://perma.cc/4UNV-BPHE].

81. *Id.*

82. The recently passed General Data Protection Regulation ("GDPR") in the European Union may affect how future privacy policies are formulated regarding "personal data," which is data that can be directly or indirectly related back to an individual, including names and location data. Regulation 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR], art. 4(1), 2016 O.J. (L 119) 33 (EU). However, it is not clear that all types of smart car data will fall under the protection of the GDPR. *Cf.* Luke Irwin, *The GDPR: What Exactly is Personal Data?,* IT GOVERNANCE (Feb. 7, 2018), https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data [https://perma.cc/BQ6T-ZET7]. The GDPR also seeks to raise the bar regarding adequate notice and consent. *See* Regulation 2016/679, GDPR, art. 7, 2016 O.J. (L 119) 37 (EU).

83. *About Automotive Privacy*, ALL. OF AUTO. MFRS., https://autoalliance.org/connected-cars/automotive-privacy/ [https://perma.cc/A72U-4TJ6].

84. *Consumer Privacy Protection Principles*, ALL. OF AUTO. MFRS. & ASS'N OF GLOB. AUTOMAKERS 2–3 (Nov. 12, 2014), https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf [https://perma.cc/TX7X-BT3G].

85. *Id.* at 7.

86. *Id.* at 8.

such information "only as needed for legitimate business purposes."[87] As for "access," automakers commit to offer consumers reasonable means to review and correct "Personal Subscription Information."[88]

However, these *privacy* principles actually do very little for the consumer regarding data *ownership*. First, disclosure in and of itself does not provide any ownership rights in the data. Second, no affirmative consent is required if the use of data is "reasonably necessary to protect the safety, property, or rights of [automakers]" or "for internal research or product development."[89] Third, the term "legitimate business purposes" is left undefined and could easily encompass any type of profit-making use of consumer data. Lastly, the only type of data that consumers will have access to is "Personal Subscription Information," which is only information related to the registration process, such as the consumer's name, contact information, and credit card information.[90] Compared to the vast varieties of data that a smart car can collect, as outlined in Part II, "Personal Subscription Data" is but a drop in the bucket. Other collected data will not necessarily be made accessible to consumers. The automotive industry-wide privacy principles are no more than a ruse to convince policymakers that the industry is self-regulating and does not need to be further regulated in regard to consumer data.[91]

That is not to completely discredit all industry-crafted privacy policies and terms of use. In general, policies and terms can provide consumers with assurances and rights regarding their data and keep companies accountable to what is represented in those policies and terms. For example, if a company fails to follow through on its privacy policies, the Federal Trade Commission is authorized to bring an enforcement action under Section 5 of the Federal Trade Commission Act, which prohibits "unfair and deceptive acts and practices."[92] However, this type of enforcement is difficult to do at scale.[93] Most FTC enforcement actions end up as consent decrees between the agency and the company, with very few punitive damages or fines.[94]

---

87. *Id.* at 11.

88. *Id.*

89. *Id.* at 9.

90. *Id.* at 5.

91. *See, e.g.*, Steve Hoffenberg, *Automotive Privacy Protection Principles Don't Go Far Enough*, VDC RESEARCH (Nov. 14, 2014), https://www.vdcresearch.com/News-events/iot-blog/2014/automotive-privacy-protection-principles.html [https://perma.cc/CD3J-CTBT].

92. *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/6ZQU-BHSJ]. Equivalent agencies at the state level could also pursue enforcement actions under state law.

93. Interview with David O'Brien, Senior Researcher, Berkman Klein Center, in Cambridge, Mass. (Jan. 17, 2018).

94. *Id.*

Future smart car privacy policies and terms of use could follow the general structure of the Automakers Alliance privacy principles. Most likely, consumers will have no power to negotiate for different terms regarding the data that is collected about them. They may have no choice but to accept the terms of use of the software installed in their smart cars, unless they decide to forgo using a smart car completely. In a regime governed primarily by contractual law, namely privacy policies and terms of use, automakers or service providers will be able to secure themselves as the de facto owners of smart car data, and thus — in accordance with the Coase Theorem — they will be able to extract most of its economic benefits.

IV. CONCLUSION

Who owns the data generated by your smart car? Most likely, the company that made your smart car does. Although the consumer owns the smart car itself, data collected by the vehicle cannot be directly "owned" like traditional intellectual property. Instead, the rights to access, limit access to, use, and destroy data are likely the closest proxies for "ownership." The smart car manufacturer will usually own the copyright of the software that envelops smart car data, and copyright law likely protects that software from unauthorized uses. Consumers might be able to get a regulatory exemption to allow them to bypass proprietary smart car software and access the data, but such an exemption would not give consumers the right to economically exploit the data. There are also currently no industry-specific statutes that govern smart car data ownership, so auto manufacturers can craft privacy policies and terms of use in their own favor, maintaining their exclusive ability to access and use smart car data. Thus, the current legal landscape suggests that all smart car data collected about the consumer, his location, driving behavior, and vehicle are all essentially owned by the smart car company.

It is possible for the law to change rapidly in the near future. High-profile data usage scandals, such as the recent one involving Facebook and Cambridge Analytica,[95] might raise public and legislative awareness about how consumer data can be exploited and who sees financial gains from such exploitation. Perhaps legislators will start to lean towards a data ownership model like the one applied to EDR data or a heavily regulated regime like HIPAA. On the other hand, as technology seeps deeper into everyday life, consumers may become more accustomed to, or

95. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/5S7D-M2NZ].

even blasé about, having data constantly being collected about their actions.[96]

Concerns about data privacy will likely shape the legal landscape, but such a focus on data *privacy* obscures the significance of data *ownership*. If the auto industry maintains exclusive access to valuable smart car data, then consumers, government entities, or other businesses that want to utilize smart car data will have to negotiate with the industry. According to the Coase Theorem, this will allow the industry to extract value from other parties who desire to use smart car data. On the other hand, if the law gives consumers property-like interests in smart car data, then that value can be extracted by consumers instead. It is important to remember that the creation of smart car data will likely increase the proverbial "economic pie." Whoever owns smart car data will get to take the first and biggest bite out of that "extra pie."

96. *See, e.g.*, Cara Bloom, Joshua Tan, Javed Ramjohn & Lujo Bauer, *Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles*, PROCEEDINGS OF THE 13TH SYMP. ON USEABLE PRIVACY AND SEC., July 12–14, 2017, at 357, 358, https://www.usenix.org/system/files/conference/soups2017/soups2017-bloom.pdf [https://perma.cc/Q397-PEKG] (showing that 46% of people would not spend five minutes to opt-out of being identified by autonomous vehicles sensors in public spaces); John Fleming & Amy Adkins, *Data Security: Not a Big Concern for Millennials*, GALLUP (June 9, 2016), https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx [https://perma.cc/XPB2-QKHR].