Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2018

Autonomy in the Age of Autonomous Vehicles

Michael Mattioli
Indiana University Maurer School of Law, mmattiol@indiana.edu

ARTICLE

AUTONOMY IN THE AGE OF AUTONOMOUS VEHICLES

MICHAEL MATTIOLI[1]

CONTENTS

INTRODUCTION

On March 18, 2018, a 49-year-old woman walking her bicycle across a street in Tempe, Arizona, was struck and killed by a car operated by the ride-sharing company, Uber.[2] Although about 40,000 people in the United States die in car accidents each year, this death was unique: the victim was the first pedestrian killed by an autonomous car.[3] In the days that followed, authorities tried to understand how the car had made its fatal decision. Inconveniently, they had to rely upon Uber's willingness to share data the vehicle had recorded around the time of the accident.[4] Because autonomous vehicle makers are not required to

[1] Professor of Law, Indiana University Maurer School of Law (Bloomington). I gratefully thank the organizers and panelists of the Boston University Journal of Science and Technology Law's Governing the Internet: Public Access, Private Regulation Symposium.

[2] Aarian Marshall, *Uber's Self-Driving Car Just Killed Somebody. Now What?*, WIRED (Mar. 19, 2018), https://www.wired.com/story/uber-self-driving-car-crash-arizona-pedestrian/ [hereinafter Marshall, *Uber Kills Pedestrian*]; Daisuke Wakabayashi, *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*, N.Y. TIMES (Mar. 19, 2018), https://nyti.ms/2GMaWfO.

[3] Marshall, *Uber Kills Pedestrian*, *supra* note 2; Neal E. Boudette, *Tesla's Self-Driving System Cleared in Deadly Crash*, N.Y. TIMES (Jan. 19, 2017) https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html; Wakabayashi, *supra* note 2.

[4] Marshall, *Uber Kills Pedestrian*, *supra* note 2.

disclose accident data, companies like Uber make such data difficult for outsiders, including investigators, to independently access and interpret.[5]

In 2016, federal investigators were similarly dependent on Tesla to help them understand how a passenger in one of its autonomous vehicles had died on a stretch of Florida highway.[6] Without that data, only the most bare facts were known: the victim was a former Navy SEAL; he was forty years old; his Tesla Model S collided with a tractor-trailer hauling blueberries; he probably died instantly.[7] Only with Tesla's cooperation were federal investigators able to access and make sense of data that told the deeper story. (The data revealed the driver was at least partly at fault.)[8] Following a fatal 2018 crash, a spokesperson for the National Transportation Safety Board stated that the agency was "unhappy" with Tesla for selectively publicizing certain facts which appeared to exculpate the company before investigators had completed their analysis of all of the crash

[5] *See, e.g.*, Joseph A. Gregor, Nat'l Transp. Safety Bd., HWY16FH018, Driver Assistance System - Factual Report (Jun. 20, 2017) https://dms.ntsb.gov/pubdms/search/document.cfm?docID=453441&docketID=59989&mkey=93548 [https://perma.cc/F3YR-LNDH] ("But the vast majority [of data recovered from the vehicle], including the vehicle log files containing all of the parametric data discussed in this report, was stored in a proprietary binary format that required the use of in-house manufacturer software tools for conversion into engineering units.").

[6] This statement is supported generally by reports of Tesla's willingness to share data with investigators, and more specifically documents in the NTSB docket. *See id.* For more examples showing the public's reliance on Tesla in this respect, see, for instance, Amy Martyn, *Tesla blames drivers who wreck its cars but won't hand over a court order*, CONSUMER AFFAIRS (May 30, 2018), https://www.consumeraffairs.com/news/tesla-blames-drivers-who-wreck-its-cars-but-wont-hand-over-crash-data-without-a-court-order-053018.html [https://perma.cc/T9CQ-UWG7] (reporting accounts of the company's unwillingness to share data).

[7] Rachel Abrams & Annalyn Kurtz, *Joshua Brown, Who Died in Self-Driving Accident, Tested Limits of His Tesla*, N.Y. Times (July 1, 2016), https://www.nytimes.com/2016/07/02/business/joshua-brown-technology-enthusiast-tested-the-limits-of-his-tesla.html; Jordan Golson, *Read the Florida Highway Patrol's Full Investigation into the Fatal Tesla Crash*, THE VERGE (Feb. 1, 2017 1:13 PM), https://www.theverge.com/2017/2/1/14458662/tesla-autopilot-crash-accident-florida-fatal-highway-patrol-report [https://perma.cc/B8NP-36AV].

[8] Ashley Halsey III, *NTSB Says Driver in Fatal Tesla Crash was Overreliant on the Car's 'Autopilot' System*, WASH. POST (Sep. 12, 2017), https://www.washingtonpost.com/local/trafficandcommuting/ntsb-says-driver-in-fatal-tesla-crash-was-overreliant-on-the-cars-autopilot-system/2017/09/12/38e5f130-9730-11e7-82e4-f1076f6d6152_story.html?utm_term=.22baac62063a [https://perma.cc/T7TA-RVQT]; Junko Yoshida, *Fatal Tesla Crash: That's Not All, Folks*, EE TIMES (June 27, 2017), https://www.eetimes.com/author.asp?doc_id=1331950. *But see* Aarian Marshall, *Tesla Bears Some Blame for Self-Driving Crash Death, Feds Say*, WIRED (Sept. 13, 2017, 7:00 AM), https://www.wired.com/story/tesla-ntsb-autopilot-crash-death/ [https://perma.cc/4BP3-WPLQ].

data.[9] These episodes indicate a tension between the public's interest in independently evaluating the risks of autonomous vehicles and the value automakers derive from controlling the disclosure of data.

These tragedies and the data-intensive investigations that followed have also led some experts to push for greater data-sharing *between competing automakers*. Data describing a vehicle's location, speed, trip history, external road conditions, and the like could improve safety in two ways: first, by sharing such data wirelessly while on the road, autonomous vehicles could intelligently coordinate to better avoid collisions;[10] second, by sharing data about crashes and other important road events *after* they occur, automakers could make all cars smarter and safer over time.[11] Because such data can give individual automakers a competitive edge, however, such data-sharing is not widely taking place. In light of this, some experts are considering whether automakers should be legally required to share data, and if so, what these new rules of the road should look like.[12]

As the debate over passenger safety revs up, a second controversy concerning passenger autonomy has begun. Some auto manufactures, wireless telecoms, online service providers, and advertisers want to make autonomous vehicles the next great platforms for ad-funded media and services.[13] To do so, they hope to repackage and sell (or otherwise monetize) some of the same data at the heart of

[9] Faiz Siddiqui, *NTSB 'unhappy' with Tesla release of investigative information in fatal crash*, WASH. POST (April 1, 2018), https://www.washingtonpost.com/news/drgridlock/wp/2018/04/01/ntsb-unhappy-with-tesla-release-of-investigative-information-in-fatal-crash/?utm_term=.32d568353db9 [https://perma.cc/4UDL-6A69].

[10] Lucas Mearian, *Feds Want Cars to Talk to Each Other to Avoid Crashes*, COMPUTERWORLD (Dec. 15, 2016), https://www.computerworld.com/article/3151105/car-tech/feds-want-cars-to-talk-to-each-other-to-avoid-crashes.html [https://perma.cc/F89E-84US].

[11] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN, U.S. DEP'T TRANSP., FEDERAL AUTOMATED VEHICLES POLICY 17-18 (2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf [https://perma.cc/X83X-3952].

[12] *See* Sharing Automated Vehicle Records with Everyone for Safety ("SHARES") Act, H.R. 3430, 115th Cong. (2017) (providing from the establishment of a framework to support such data-sharing); Ryan McCauley, *3 Concerns Automakers Have With California's Autonomous Vehicle Regulations*, GOVTECH (Oct. 26, 2016), http://www.govtech.com/fs/3-concerns-automakers-have-with-californias-autonomous-vehicle-regulations.html [https://perma.cc/LY46-CX7V] (reporting industry concerns over the possibility of such data-sharing requirements); Jamie Williams & Peter Eckersley, *Some Easy Things We Could Do to Make All Autonomous Vehicles Safer*, ELEC. FRONTIER FOUND. (Mar. 29, 2018), https://www.eff.org/deeplinks/2018/03/some-easy-things-we-could-do-make-all-autonomous-cars-safer-faster [https://perma.cc/AZH4-HHY4].

[13] *The Connected Car Opportunity*, EMARKETER (Jun. 22, 2017), https://www.emarketer.com/Article/Connected-Car-Opportunity/1016065 [https://perma.cc/VB49-6F85].

the debate over passenger safety.[14] Such data includes, for instance, vehicle location, speed, heading, and passenger driving habits. Privacy experts warn that this would open the door to harmful new forms of commercial surveillance.[15]

These controversies over safety and privacy have been unfolding independently, but they are deeply intertwined. They implicate some of the same underlying data—and consequently, some of the same underlying policy issues. Consider, for instance, vehicle location. Congress is now considering a bill that would allow drivers to opt-out of vehicle location tracking altogether—a measure that would, if passed into law, appear to conflict directly with a second pending Congressional bill that would require mandatory data-sharing between automakers.[16] Moreover, "consumer privacy" might offer a convenient and plausible excuse for automakers who are reluctant to share vehicle safety data purely for competitive reasons. In the autonomous vehicle industry, privacy, safety, competition, and commerce all seem to be headed for gridlock.[17]

Analogous dilemmas exist outside the auto industry. I recently examined a similar quandary concerning data in the field of healthcare, for instance.[18] On one side were health advocates who argued that hospitals should pool patient treatment records to advance disease research; on the other side were privacy experts who cautioned that such data-sharing could open the door to widespread disclosure of confidential patient information. The problem seemed intractable. Through discussions with various stakeholders, however, I learned that viewing the situation in terms of "patient health versus privacy" was facile. The types of data, the parties interested in it, and their individual motivations were far more varied than they appeared at first glance. This discovery pointed the way to new potential solutions. My aim in conducting the study was to show the virtues of a holistic, ethnographic approach to examining data policy problems.

[14] *See infra* Part II.

[15] Marshall, *supra* note 8; *see also* Jamie Condliffe, *Why Some Autonomous Cars Are Going to Avoid the Internet*, MIT TECH. REV. (Jan. 10, 2017), https://www.technologyreview.com/s/603339/why-some-autonomous-cars-are-going-to-avoid-the-internet/amp/ (discussing security concerns) [https://perma.cc/7L2H-XRHK]; 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/ [https://perma.cc/V9J4-FZY9] (discussing the security vulnerabilities of autonomous vehicles, a topic beyond the scope of this essay).

[16] Spy Car Act of 2017, S. 680, 115th Cong. (2017).

[17] *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY (2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf [https://perma.cc/X83X-3952] (highlighting the importance of data-sharing and suggesting that it should be mandatory, while on the next page expressing the importance of consumer choice concerning data collection).

[18] Michael Mattioli, *The Data-Pooling Problem*, 32 BERKELEY TECH. L.J. 179 (2017).

This essay takes a small first step in the same direction with the driverless data dilemma. The goals of promoting privacy, safety, competition, and commerce are all so deeply intertwined, I argue, that they must be addressed together. This argument could easily be misread as a critique of earlier scholarly works that have focused on individual policy goals. To the contrary, other scholars' insightful and valuable work is part of this essay's foundation. This short essay does not attempt to solve the problem. Instead, it presents a descriptive snapshot of the current state of play, and closes by raising a set of questions stemming from my analysis. I hope these questions will prompt useful discussions among policy experts and the public.

Part I explains what types of data autonomous vehicles collect. Part II explains how this data can improve public safety, and the value automakers derive from secrecy. Part III explores how some of the same data may be used for marketing purposes in the future. Part IV examines the interplay between the themes in Parts II and III and presents a set of unexplored questions intended to stimulate policy discussions.

I. SAFETY AND SECRECY

Despite automakers' ongoing efforts to make vehicles safer, car travel is relatively dangerous. Of the over three-hundred and twenty million people living in America in 2017,[19] about 40,000 died and 4.5 million were injured in car accidents.[20] Human error is overwhelmingly to blame.[21] From an evolutionary perspective, our poor collective driving record might seem understandable: What in our species' history, after all, could have conditioned us to make split-second

[19] *Population and Housing Estimates*, U.S. CENSUS BUREAU https://www.census.gov/programs-surveys/popest.html [http://perma.cc/6FL2-2A7D] (last visited Apr. 10, 2018) (reporting approximately 327,511,673 living in the United States as of April 10, 2018 at 10:30 PM Eastern).

[20] Motor-vehicle related deaths routinely number in the tens of thousands. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 812456, 2016 FATAL MOTOR VEHICLE CRASHES: OVERVIEW (2017) ("There were 37,461 people killed in crashes on U.S. roadways during 2016, an increase from 35,485 in 2015."); STATISTICS DEP'T, NAT'L SAFETY COUNCIL, *NSC Motor Vehicle Fatality Estimates*, NAT'L SAFETY COUNCIL, https://www.nsc.org/Portals/0/Documents/NewsDocuments/2018/December_2017.pdf (last visited Apr. 10, 2018) [http://perma.cc/X5KX-37EB] (showing that there were 40, 1000 motor-vehicle deaths in 2017). By way of comparison, there were zero deaths in commercial airlines in 2017. David Shepardson, *2017 safest year on record for commercial passenger air travel: groups*, REUTERS (Jan. 1, 2018, 1:54 PM), https://www.reuters.com/article/us-aviation-safety/2017-safest-year-on-record-for-commercial-passenger-air-travel-groups-idUSKBN1EQ17L [https://perma.cc/PMX7-U7F8] ("Airlines recorded zero accident deaths in commercial passenger jets last year, according to a Dutch consulting firm and an aviation safety group that tracks crashes . . . .").

[21] *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Automated Vehicles for Safety*, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety [https://perma.cc/B7KA-HMDK] ("94 percent of serious crashes are due to human error.").

decisions while hurtling across the countryside at seventy-five miles-per-hour? Less understandable, though, is why so many drivers make matters worse by taking the wheel drunk and distracted. These two activities caused 10,497 and 3,450 deaths, respectively, in 2016 alone.[22]

In the United States today, dozens of companies are testing autonomous technologies that hold the promise of far greater safety.[23]These computer-controlled vehicles have "eyes" that can see the world with remarkable clarity: 360-degree cameras can see hazards a person can't; sonar and radar can see in the dark; spinning lasers can cut through fog and darkness to map a vehicle's surroundings; and GPS sensors give autonomous vehicles a sense of geospatial location and heading that humans innately lack. This data is delivered to on-board computers running software algorithms that predict collisions, merges, lane changes, and so on.[24] The software then directs the vehicle to move accordingly.[25] Autonomous vehicles are already able to match the safety of most human drivers in some road settings—and without ever doing so drunk, distracted, drowsy, or angry.

[22] *USDOT Releases 2016 Fatal Traffic Crash Data*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (Oct. 6, 2017), https://www.nhtsa.gov/press-releases/usdot-releases-2016-fatal-traffic-crash-data [http://perma.cc/EKY5-SXXC].

[23] *See* Aarian Marshall, *To Save The Most Lives, Deploy (Imperfect) Self-Driving Cars ASAP*, WIRED (Nov. 7, 2017, 12:01 AM), https://www.wired.com/story/self-driving-cars-rand-report/ [https://perma.cc/PEC6-TCZ6] (reporting 43 companies in California alone); Kirsten Korosec, *Here's Where the 10 Federal Self-Driving Car Test Sites Are*, FORTUNE (Jan. 21, 2017) http://fortune.com/2017/01/20/self-driving-test-sites/ [https://perma.cc/V24K-8HVH] (announcing that ten sites throughout the U.S. had been selected by the Department of Transportation for "developing and testing self-driving car technology"). *See also* Alison DeNisco Rayome, *Dossier: The leaders in self-driving cars*, ZDNET (Feb. 1, 2018, 9:57 PM), https://www.zdnet.com/article/dossier-the-leaders-in-self-driving-cars/ [https://perma.cc/BW4C-5ABQ] (listing "leaders" in the development of self-driving cars, which can be taken as illustrative of how ubiquitous those companies — from General Motors to Waymo — believe autonomous vehicles may one day be).

[24] *See, e.g.*, Cade Metz, *How Driverless Cars See the World Around Them*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/how-driverless-cars-work.html (indicating role of on-board computer situated in trunk) [hereinafter Metz, *How Driverless Cars See the Word*]; Cade Metz, *Competing with the Giants in the Race to Build Self-Driving Cars*, N.Y. TIMES (Jan. 4, 2018), https://www.nytimes.com/2018/01/04/technology/self-driving-cars-aurora.html (discussing software installed in cars and various approaches to algorithmic design) [hereinafter Metz, *Competing with the Giants*]; Todd Spangler, *Self-driving cars programmed to decide who dies in a crash*, USA TODAY (Nov. 23, 2017), https://www.usatoday.com/story/money/cars/2017/11/23/self-driving-cars-programmed-decide-who-dies-crash/891493001/ [https://perma.cc/WA5X-3UVK]; John Patrick Pullen, *You Asked: How Do Driverless Cars Work?*, TIME (Feb. 24, 2015), http://time.com/3719270/you-asked-how-do-driverless-cars-work/ [https://perma.cc/5ZDS-8DVF].

[25] *Id.*

The table below lists some of the most common types of data captured by autonomous vehicles now being tested:

Table 1: Common Types of Autonomous Vehicle Data and Sources[26]

Data Gathered	Source(s) and Notes
Vehicle location	GPS sensor and chipset
Local time	on-board computer
Vehicle make / model	on-board computer
Speed	on-board sensor(s)
Acceleration	on-board sensor(s)
Vehicle Roll Angle	on-board sensors
Heading	on-board compass
Braking (percentage applied)	on-board sensors
Accelerator (percentage applied)	on-board sensors
Seatbelts in use	on-board sensors
Hands on wheel	on-board sensors
Steering input (steering angle)	on-board sensors
Vehicle lights (brake, etc.)	on-board sensors

[26] In the context of this article, "sensor" refers generally to any technology installed on an autonomous vehicle with the purpose of gathering data. Thus, if a vehicle senses "hands on the wheel," it necessarily must do so with a sensor of some kind. Table 1 refers to some specific types of sensors, such as LIDAR and cameras, and alternatively defaults to the general term "sensor" to refer to a data-gathering device that isn't specified. The following sources refer to types of data, as well as specific types of sensors. Event Data Recorders, 77 Fed. Reg. 47,552, 47,557 (Aug. 9, 2012) (to be codified at 49 C.F.R. pt. 563) (listing requirements for data to be captured by event data recorders voluntarily included in many vehicles by manufacturers); Jamie Condliffe, *Lidar Just Got Way Better-But It's Still Too Expensive For Your Car*, MIT TECH. REV. (Nov. 28, 2017), https://www.technologyreview.com/s/609526/lidar-just-got-way-better-but-its-still-too-expensive-for-your-car/ [http://perma.cc/5AD3-522Y]; Cade Metz, *How Driverless Cars See the World around Them*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/how-driverless-cars-work.html; Nat'l Transp. Safety Bd., *Preliminary Report*, NTSB: DOCKET MANAGEMENT SYSTEM (June 15, 2017), https://dms.ntsb.gov/public/59500-59999/59989/604690.pdf [https://perma.cc/72WK-UKPZ] (raw data shared by the NTSB in connection with Tesla vehicle crash of May, 2016); The Tesla Team, *All Tesla Cars Being Produced Now Have Full Self-Driving Hardware*, TESLA: BLOG (Oct. 19, 2016), https://www.tesla.com/blog/all-tesla-cars-being-produced-now-have-full-self-driving-hardware [https://perma.cc/3WZZ-WUMH].

Occupancy	Sensors built into seats
Environment immediately surrounding vehicle[27]	Camera array (photo and video) Lidar (light detection and ranging): using lasers, device creates a 360-degree map of the car's surroundings. Radar (radio detection and ranging): measures distance from car to surrounding objects. Sonar (sound detection and ranging)
Sound inside vehicle	in-vehicle microphone(s)
Phones connected	On-board computer (Bluetooth)
Apps in use (e.g., online music and entertainment services)	On-board computer

The data that autonomous vehicles collect has enormous value to automakers. Because highways and roads present more driving situations than a team of programmers could possibly anticipate, the software directing autonomous vehicles relies upon artificial intelligence—neural networks[28] and machine learning algorithms—that can reason in some ways like a human mind.[29] Software developers "teach" these systems by feeding them copious examples of good and bad decisions—"training data"—from which the algorithm can learn and improve.[30] For nearly all autonomous automakers, the sources of this training data are the very cars they have already put out on the roads.[31] An automaker's fleet of cars captures data, which in turn teaches the fleet before it goes out again to capture more data, and so on. In the auto industry, this virtuous cycle is called "fleet learning."[32]

[27] Metz, *How Driverless Cars See the Word*, *supra* note 24.

[28] Metz, *Competing with the Giants*, *supra* note 24.

[29] Metz, *How Driverless Cars See the Word*, *supra* note 24.

[30] *See* Levi Tillemann & Colin McCormick, *Will Driverless-Car Makers Learn to Share?*, NEW YORKER (Sept. 25, 2016), https://www.newyorker.com/business/currency/will-driverless-car-makers-learn-to-share [https://perma.cc/EPK5-6J3H]; *see also* Michael Dempsey, (H)edge cases in Autonomous Vehicles, MEDIUM (Mar. 9, 2016) https://medium.com/frontier-tech/h-edge-cases-in-autonomous-vehicles-37f75fe63b56.

[31] Tillemann & McCormick, *supra* note 30.

[32] *Id.*

For all their sophistication, autonomous vehicles remain inferior to most human drivers. Recent commentary has highlighted the shortcomings of Uber's vehicles in handling "edge cases"—uncommon road situations that are difficult to foresee and that only show up in huge sets of training data—lengthy road signs, interpreting subtle non-verbal cues from other drivers and so forth.[33] According to Brandon Schoettle, a transportation expert at the University of Michigan, although these vehicles might see the world with amazing detail, humans still understand it better. In a recent interview with Wired, Schoettle commented, "You're probably safer in a self-driving car than with a 16-year-old, or a 90-year-old . . . . But you're probably significantly safer with an alert, experienced, middle-aged driver than in a self-driving car."[34]

The way to make autonomous vehicles safer, some experts believe, is to require vehicle manufacturers to share the data captured by their fleets. In a guidance document published in 2016, the U.S. Department of Transportation (USDOT) and the National Highway Traffic Safety Administration (NHTSA) suggested this idea.[35] In a carefully researched law journal student note, Jesse Krompier argued that the NHTSA should enact rules mandating the sharing of automation data between automakers to ensure consumer safety.[36] A recent editorial in the Boston Globe expressed a similar view, asking rhetorically, "Do we want makers of autonomous vehicles to pitch their product based on being less likely to mow down a pedestrian — or on other features, like comfort, range,

[33] Daisuke Wakabayashi, *Uber's Self-Driving Cars Were Struggling before Arizona Crash*, N.Y. TIMES (Mar. 23, 2018), https://www.nytimes.com/2018/03/23/technology/uber-self-driving-cars-arizona.html [https://perma.cc/6JMQ-3W6D].

[34] Aarian Marshall, *Puny Humans Still See the World Better Than Self-Driving Cars*, WIRED (Aug. 5, 2017), https://www.wired.com/story/self-driving-cars-perception-humans/.

[35] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY 18 (2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf [https://perma.cc/8D24-U5AQ] ("[E]ach entity should develop a plan for sharing its event reconstruction and other relevant data with other entities. Such shared data would help to accelerate knowledge and understanding of HAV performance, and could be used to enhance the safety of HAV systems.").

[36] Jesse Krompier, Note, *Safety First: The Case for Mandatory Data Sharing as a Federal Safety Standard for Self-Driving Cars*, 2017 U. ILL. J.L. TECH & POL'Y 439, 455-59 (2017) ("Consumers should not have to choose one self-driving car over another based on which one has a better understanding of the driving environment and the dynamic objects on the road."). Other commentators have likewise argued that autonomous vehicles should be made as safe as possible in a short time span. *See* Ashley Halsey III, *How Safe Is 'Safe Enough' to Put Driverless Cars on the Nation's Roadways?*, WASH. POST (Dec. 10, 2017), https://www.washingtonpost.com/local/trafficandcommuting/how-safe-is-safe-enough-to-put-driverless-cars-on-the-nations-roadways/2017/12/10/9a1aa348-d519-11e7-b62d-d9345ced896d_story.html?utm_term=.ecc0b8c46325.

or whether the speed of the in-car Wi-Fi is fast enough for five passengers to stream five different Netflix shows?"[37]

Experts have also argued that automakers should disclose autonomous vehicle crash data to the public. In a 2016 statement issued to the NHTSA, for instance, a consumer interest group wrote, "[f]ull public access to this test vehicle data, especially when a crash occurs or a car is incapable of handling a situation on the road, is indispensable to any meaningful evaluation of whether autonomous vehicles are safe."[38] Additionally, an executive at Consumer Reports recently commented to Congress that, "[r]ight now, the safety benefits of autonomous driving are entirely speculative and based on data held internally. Regulators and consumers deserve to know the basis that companies use to determine that an automated technology is safe. This kind of disclosure would only help companies build trust in their products."[39]

Although it might make cars safer, mandatory data-sharing seems to be at odds with the competitive landscape of the autonomous vehicle industry. Automakers developing autonomous vehicles rely heavily on trade secrets. These companies have vocally opposed sharing vehicle data, for fear that it could give competitors a leg up.[40] For example, in a letter to the California Department of Motor Vehicles (DMV) the director of safety for Google's autonomous vehicle program wrote that certain data describing the limits of their autonomous technology "is highly confidential, particularly during the testing phase before a product is brought to market."[41] He added, "[p]ublic disclosure of this information could cause great financial harm to Google."[42] In a similar letter to the California DMV, the CEO of Uber expressed concerns about a proposed rule that would have required the disclosure of testing data, writing "[t]he Proposed Regulations should be revised to recognize that this information can be a confidential trade secret, which should not be subject to disclosure."[43] TechCrunch, a popular technology news website, has painted a similar picture:

[37] Scott Kirsner, *For the Sake of Safe Self-Driving Cars, Companies Need to Share Data*, BOS. GLOBE (Mar. 31, 2017), https://www.bostonglobe.com/business/2017/03/31/for-sake-safe-self-driving-cars-companies-need-share-data/itF4HUFL6A1HQMSeDaa5zI/story.html.

[38] CONSUMER WATCHDOG, Comment Letter on Federal Automated Vehicles Policy, DOT Docket No. NHTSA-2016-0090 (Nov. 22, 2016), http://www.consumerwatchdog.org/resources/nhtsacomments11-22-16.pdf [https://perma.cc/U3NH-Y4X2].

[39] *Disrupter Series: Self-Driving Cars: Hearing before the Subcomm. on Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce*, 114th Cong. 55 (2016) (statement of Laura MacCleery, Vice President, Consumer Policy and Mobilization, Consumer Reports), http://docs.house.gov/meetings/IF/IF17/20161115/105416/HHRG-114-IF17-Wstate-MacCleeryL-20161115.pdf [https://perma.cc/TG5T-YUTL].

[40] Mark Harris, *These are the secrets Google wanted to keep about its self-driving cars*, QUARTZ (Aug. 21, 2014) https://qz.com/252817 [https://perma.cc/A59R-BDPF].

[41] *Id.*

[42] *Id.*

[43] Letter from Anthony Levandowski, Vice-President, Engineering, Uber, to Brian Soublet, Deputy Director and Chief Counsel, Cal. Dep't Motor Vehicles, (Apr. 24, 2017) (on file

Uber, Lyft and GM have all separately pointed to the vast stores of driving data collected by their respective fleets as key competitive advantages in the race to develop truly effective autonomy. And of all the data used to train these systems — information related to how autonomous vehicles handle challenging conditions or actual impact events — might be most valuable in terms of creating a really robust, adaptable self-driving car.[44]

In a collection of public comments submitted to the NHTSA in 2016, many automakers similarly opposed the suggestion of a mandatory data-sharing rule.[45]

Recent high-profile trade secret lawsuits corroborate the importance of secrecy in the autonomous vehicle industry. In 2017, Waymo — a subsidiary of Google's parent company, Alphabet — sued Uber for misappropriation of trade secrets.[46] The dispute stemmed from Uber's hiring of Anthony Levendowski, the former head of Waymo's autonomous vehicle efforts.[47] Waymo alleged in the suit that Levendowski had copied a collection of trade secrets to a personal hard drive before leaving the company, and that those technologies either had been, or would inevitably be, wrongfully used by Uber.[48] The companies settled the dispute following the discovery stage of litigation, with Uber agreeing not to use Waymo trade secrets in its autonomous vehicle program, and to transfer an equity share in Uber worth approximately 245 million dollars to Waymo.[49] As of this writing, a second trade secret lawsuit involving the automakers Faraday Future and Evelozcity is unfolding in California.[50] Although the trade secrets in these two disputes have not been publicized, they relate generally to data sensors and related software.[51] Both the settlement in Uber v. Waymo and the continued conflict between Faraday Future and Evelozcity suggest trade secrecy is important to this young industry.

Automakers' possessiveness over vehicle data is understandable. Such data is not only useful for artificial intelligence ("AI") training, but it is also costly to

with Cal. Dep't Motor Vehicles), https://www.dmv.ca.gov/portal/wcm/connect/66f80f21-8faf-4ec7-a563-4689fa0b7524/Uber.pdf?MOD=AJPERES [https://perma.cc/GTQ9-LETK].

[44] Kate Conger, *Federal Policy for Self-Driving Cars Pushes Data Sharing*, TECH CRUNCH (Sept. 20, 2016), http://tcrn.ch/2cspFyY [https://perma.cc/7KAB-B755].

[45] Jeff Plungis, *Should Developers of Driverless Cars Share Test Data?*, CONSUMER REP. (Dec. 8, 2016) https://www.consumerreports.org/autonomous-driving/should-developers-of-driverless-cars-share-test-data/ [https://perma.cc/HWD9-ZTMK].

[46] Waymo LLC v. Uber Tech., Inc., No. C 17-00939 WHA, 2017 WL 2123560, at *1 (N.D. Cal. May 15, 2017).

[47] *Id.*

[48] *Id.*

[49] Aarian Marshall, *Uber and Waymo Abruptly Settle for $245 Million*, WIRED (Feb. 9, 2018, 12:17 PM) https://www.wired.com/story/uber-waymo-lawsuit-settlement/ [https://perma.cc/2GB6-PLK7] [hereinafter Marshall, *Uber and Waymo*].

[50] Orrick – Trade Secrets Grp., *Automation of Our Auto Nation: New Tech Requires A New Look At Trade Secret Laws*, JDSUPRA, (Feb. 12, 2018), https://www.jdsupra.com/legal-news/automation-of-our-auto-nation-new-tech-54948/ [https://perma.cc/84DT-PTBX].

[51] Marshall, *Uber and Waymo*, *supra* note 49; Orrick, *supra* note 50.

gather because it requires deploying vehicles on real roads.[52] Companies that have invested heavily in capturing such data might have few incentives to share with companies that have not gathered useful data of their own—quite literally a "free-rider" problem. Moreover, because reverse-engineering is permissible under federal and state trade secret laws, a competitor might be able to use such data to reverse-engineer a valuable algorithm maintained as a trade secret.[53] Finally, the data captured by a vehicle might expose shortcomings in its design, leading to fewer sales.

At the same time, few would seriously challenge the importance of protecting the public's safety. Indeed, consumer safety groups aren't the only ones pushing for data-sharing. Apple, which has invested heavily in developing technologies for autonomous vehicles,[54] recently urged the NHTSA to set up a framework for sharing such data, writing, "companies should share de-identified scenario and dynamics data from crashes and near misses."[55] Congress, meanwhile, is currently considering a bill that would aid the NHTSA in establishing such a framework—The Sharing Automated Vehicle Records with Everyone for Safety Act (SHARES Act).[56] The House of Representatives Committee on Energy and Commerce explains that this bill, in part,

> establishes a committee within NHTSA for a two-year period to develop a framework that allows manufacturers of [highly automated vehicles] to share relevant, situational information related to any testing event on public streets that results in damage to the test vehicle or any occupant thereof and validation of such vehicles in a manner that does not risk public disclosure of such information or disclosure of confidential business information.[57]

[52] *See* Kyle Vogt, *Why testing self-driving cars on the challenging roads of San Francisco is necessary*, RECODE, (Oct. 3, 2017, 3:45 PM) https://www.recode.net/2017/10/3/16413068/testing-self-driving-cars-san-francisco-challenging-necessary [https://perma.cc/YKY5-GY7T].

[53] *See* M. Gethsiyal Augasta & T. Kathirvalavakumar, *Reverse Engineering the Neural Networks for Rule Extraction in Classification Problems*, 35 NEURAL PROCESSING LETTERS 131, 132 (2012).

[54] Andrew J. Hawkins, *Here's a closer look at Apple's secret self-driving car*, The Verge, (Oct. 18, 2017) https://www.theverge.com/2017/10/18/16496182/apple-self-driving-car-project-titan-sensor-lidar [https://perma.cc/Y2R5-455U].

[55] Plungis, *supra* note 45.

[56] Sharing Automated Vehicle Records with Everyone for Safety Act (SHARES Act) H.R. 3430, 115th Cong. (2017).

[57] Memorandum from U.S. H.R. Comm. on Energy and Commerce Majority Staff to Members of Subcomm. on Dig. Commerce and Consumer Prot., Hearing entitled "Self-Driving Vehicle Legislation" (June 23, 2017), http://docs.house.gov/meetings/IF/IF17/20170627/106182/HHRG-115-IF17-20170627-SD002.pdf [https://perma.cc/5EBH-M2EN].

An uncomfortable question underlies this debate: How safe is safe enough?[58] If the law required automakers to share event data with each other, competition over such features would likely be dampened. However, the auto industry as a whole might achieve an adequate level of safety more quickly than it would under competitive conditions. On the other hand, an industry in which automakers fiercely compete over driving safety features might yield safety innovations that, in the long term, make the public safer than it would be under a data-sharing regime. The cost, however, could be more dangerous vehicles in the near term. In short, vehicle data-sharing carries short- and long-term costs and benefits. The next part explains an additional challenge: the same data that can make us safer may also be used to compromise our privacy.

II. PRIVACY AND COMMERCE

Imagine a summer evening in the near future. You have just left your office and slip into your new autonomous car. As the vehicle gracefully exits the parking garage, you text your family and read the day's news on a tablet built into the dashboard. While scanning a news story, you see a colorful ad for a take-out dinner special at a local chain restaurant. Because the ad is tailored to your consumer profile and loyalty account with the restaurant, it presents a photo of your favorite item on the menu: the curly fries. You tap a button labeled "ORDER NOW." Conveniently, you don't need to tell your car to take you to the restaurant—it already knows about your order and has started along the fastest route. After you pick up dinner for your family, the car automatically begins driving you to your child's daycare. You pass some more time on the tablet and come across another ad: Verizon, your wireless data provider, is selling a new service called "Disney Everywhere." For $5 per month, Verizon will deliver unlimited streaming of select Disney programs to your car. You are seeing this ad, because Verizon has access to your vehicle's location and has deduced that you stop at a daycare after work every day. Based on this, it has guessed correctly that you're the parent of a young child. With a few taps, you sign up for Disney Everywhere. You and your child contentedly watch the Mickey Mouse Clubhouse and eat curly fries the whole ride home.

This scenario may sound like science fiction, but advertisers, the auto industry, wireless telecoms, and online content and service providers are steadily working toward it. In a 2017 report, Forrester Research warned consumers: "[g]et ready for your car to become yet another 'screen' where publishers and advertisers will compete for your attention."[59] Adweek, a leading advertising-

[58] Halsey III, *supra* note 36.

[59] LARA KOETZLE ET AL., AUTONOMOUS VEHICLES WILL RESHAPE THE GLOBAL ECONOMY: SIX TRANSFORMATIVE RIPPLE EFFECTS OF AUTONOMOUS TRANSPORT (2017), *quoted in* Ryan Felton, *Advertisers Will Inundate Your Future Autonomous Car With Ads Because Of Course They Will*, JALOPNIK (Aug. 4, 2017, 12:27 PM), https://jalopnik.com/advertisers-will-inundate-your-future-autonomous-car-wi-1797535547 [https://perma.cc/59XP-9TMT]; *see* Barry Levine, *Will Autonomous Vehicles Provide the Next Screens for Publishers and Advertisers?*,

trade publication in the US, has similarly predicted that car companies "will be in the position to collect an amazing amount of data from . . . cars and those who ride in them. . . . [S]elling data will become an increasingly bigger aspect of how car brands make money."[60]

Smartphone app developers, which already have a foothold in vehicles thanks to the ubiquity of smartphones, are seizing on the opportunities of in-vehicle advertising today. In March, 2018, the popular navigation software company, Waze, launched a service that allows businesses to display ads to nearby drivers using the Waze app.[61] On the day of the service's launch, Waze's website explained that the service will let advertisers "[t]arget drivers who are on the go near [their] business location with a meaningful local ad experience."[62] The service also gives advertisers the ability to "track" potential customers to see "exactly how many potential customers" respond to particular ads.[63]

Meanwhile, in February 2018, the Southern District of New York issued a favorable ruling to Vugo, a Minnesota company that places ads in vehicles driven for ridesharing companies like Uber and Lyft.[64] Vugo's complaint challenged the constitutionality of a local New York City law that prohibited advertising in vehicles not licensed by the city's Taxi and Limousine Commission.[65] Relying on Supreme Court precedent, the District Court sided with Vugo, opening the door to in-vehicle advertising in one of the strongest ride-sharing markets in the country.[66]

At least some vehicle manufacturers seem likely to work with third parties to share vehicle locations, trip histories, and other data necessary for in-car advertising. In March 2018, a company called Telenav was reportedly in "deep discussions" with several automakers about bringing similar ads to media displays in privately owned autonomous vehicles.[67] In a February 2018 interview, Ford's

MARTECH (Aug. 3, 2017, 2:26 PM), https://martechtoday.com/autonomous-vehicles-provide-next-screens-publishers-advertisers-201914 [https://perma.cc/J7HZ-KZQF].

[60] Thomas Bloch, *The Next Great Media Channel Is the Self-Driving Car. Will Brands Be Ready?*, ADWEEK (Oct. 30, 2017), http://www.adweek.com/agencies/the-next-great-media-channel-is-the-self-driving-car-will-brands-be-ready/amp/ [https://perma.cc/8CCK-7W3H].

[61] WAZE|LOCAL, https://www.waze.com/business/?env=am (last visited Mar. 15, 2018) [https://perma.cc/8SWR-DUTM].

[62] *Id.*

[63] *Id.*

[64] Vugo, Inc. v. City of New York, No. 15-CV-8253 (RA), 2018 WL 103339, at *1 (S.D.N.Y. Feb. 22, 2018).

[65] *Id.*

[66] *Id.*

[67] Gabrielle Coppola & David Welch, *The Car of The Future Will Sell Your Data*, BLOOMBERG (Feb. 20, 2018, 5:00 AM), https://www.bloomberg.com/news/articles/2018-02-20/the-car-of-the-future-will-sell-your-data?utm_content=tech&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social&cmpid%3D=socialflow-twitter-tech [https://perma.cc/5CZ2-AVQE].

executive director for connected vehicles and services told Bloomberg that automakers see the ability to share vehicle data—anonymized or personalized—as an important business opportunity.[68] In the same report, an industry expert told Bloomberg that "[c]armakers' ultimate objective . . . is to build a database of consumer preferences that could be aggregated and sold to outside vendors for marketing purposes, much like Google and Facebook do today."[69] "Carmakers recognize they're fighting a war over customer data," the expert added.[70] "Your driving behavior, location, has monetary value, not unlike your search activity."[71] The CEO of a software company working with GM, similarly explained to journalists that in-car advertising will be attractive to manufacturers, both because it will serve as a revenue stream, and a platform for building stronger relationships with drivers.[72]

Even if some vehicle manufacturers don't get involved in sharing vehicle data for advertising purposes, the mobile ISPs that connect our cars to the internet still may. Today, wireless firms like Verizon, AT&T, and T-Mobile reportedly have the technological ability to determine the locations of customers by means other than GPS—the distance of a caller to a cell tower or known Wi-Fi network, for instance.[73] According to a recent report in the *Wall Street Journal*, Verizon, Sprint and other ISPs repackage and sell such data to "data brokers"—companies that share useful metrics with retailers.[74] One such company called SAP, for instance, offers a product that can tell retailers detailed anonymized information such as "the age ranges and genders of people who visited a store location between 10 a.m. and noon . . . ."[75] By combining this information with web browsing and shopping data (also provided by an ISP), SAP can provide a retailer with an even more detailed portrait. Mobile ISPs may similarly be able to gather and share vehicle location information with or without an automaker's participation.

Recent steps by Congress and the FTC have made these new forms of "surveillance capitalism" possible.[76] In March 2017, Congress eliminated a set of

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] Christopher Mims, *Your Location Data Is Being Sold—Often Without Your Knowledge*, WALL STREET J. (Mar. 4, 2018), https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400.

[74] *Id.*

[75] Kate Kaye, *The $24 Billion Data Business That Telcos Don't Want to Talk About*, ADAGE (Oct. 26, 2015), http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058.

[76] *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015).

rules adopted by the FCC one year earlier that prevented internet service providers from sharing certain data with third parties unless a customer had given express permission.[77] This permitted ISPs to sell data collected from their customers, including locations, browsing histories, and shopping habits.[78] As Tom Wheeler, former chairman of the FCC recently wrote, the repeal of the 2016 FCC privacy rules "allows unrestrained sale of the personal information of any American using the internet."[79]

Similarly, the FCC's 2017 repeal of network neutrality rules could make it possible for wireless ISPs to offer highly tailored content and media packages, like the hypothetical "Disney Everywhere" service described earlier. The rules would have prevented ISPs from giving preferential treatment to certain websites or blocking others—activities that are now both allowed.[80] The rationale for the repeal, as the ISPs tell it, is that the industry needs more revenue to build infrastructure.[81] The plan is to draw that revenue by charging consumers and online service providers different rates for varying levels of service.[82] In fact, prior to the 2017 repeal, Comcast informed the FCC that the expected need for high-speed data in autonomous vehicles was a reason why network neutrality should be repealed.[83] Intel, which plans to sell computer hardware for autonomous vehicles, has also argued that high speed ("5G") networks will be important in the autonomous age.[84]

[77] S.J. Res. 34, 115th Cong. (2017); *see also* Tom Wheeler, *How the Republicans Sold Your Privacy to Internet Providers*, N.Y. TIMES, (Mar. 29, 2017), https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html.

[78] *Id.*

[79] *Id.*

[80] *See* Celia Kang, *F.C.C. Repeals Net Neutrality Rules*, N.Y. TIMES (Dec. 14, 2017), https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html.

[81] *See, e.g.*, Comcast Corporation, Comments on the Notice of Proposed Rulemaking by the FCC on Restoring Internet Freedom 26-7 (July 17, 2006), http://update.comcast.com/wp-content/uploads/sites/33/securepdfs/2017/07/2017-07-17-AS-FILED-Comcast-2017-Open-Internet-Comments-and-Appendices.pdf [https://perma.cc/Q38R-MNJH].

[82] *See* Paul Schrodt, *What the End of Net Neutrality Means for You*, TIME: MONEY (Dec. 15, 2017), http://time.com/money/5065743/how-net-neutrality-decision-affects-you/ [https://perma.cc/KM7Q-X6PR].

[83] Comcast, *supra* note 81, at 56-57. Comcast phrased the comment vaguely, leading some commentators to criticize the company for incorrectly suggesting that mobile internet connections would somehow be necessary for vehicle-to-vehicle communications safety. *See* Andrew J. Hawkins, *Why is Comcast Using Self-Driving Cars to Justify Abolishing Net Neutrality?*, THE VERGE (Jul. 18, 2017, 2:54 PM), https://www.theverge.com/2017/7/18/15990092/comcast-self-driving-car-net-neutrality-v2x-ltev [http://perma.cc/2WRM-B8TT].

[84] *Autonomous Driving*, INTEL (2017), https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/01/5G-ad-infographic.png [https://perma.cc/7CCV-PLSX].

Unsurprisingly, the prospect of widespread vehicle tracking has concerned privacy experts. Privacy law seeks, in part, to preserve individual autonomy.[85] As Dorothy Glancy explained in a recent article on privacy in autonomous vehicles,

> [i]n general, personal autonomy privacy interests focus on an individual's ability to control such matters as who knows where she is now, where will she go next, when she will depart, how she will get there and with whom, as well as who can predict or decide where, when, and how she will travel in the future.[86]

Autonomous vehicle tracking, Glancy argues, would "directly affect the autonomy of travelers by overriding individual control over who or what watches and keeps track of their movements from place to place."[87]

The Supreme Court articulated this core privacy concern vividly in the 2012 decision of *United States. v. Jones*.[88] The case dealt with whether the government's installation of a GPS device on a criminal suspect's vehicle for tracking purposes constituted a search under the meaning of the Fourth Amendment.[89] In a concurring opinion, Justice Sotomayor quoted a passage from a case she had decided earlier in her career:

> "Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[90]

The mere awareness that one's location is being tracked by the government, Justice Sotomayor reasoned, can chill our desire to associate and express ourselves freely.[91] Location tracking by invisible, sprawling networks of companies buying and selling our location data might reasonably be expected to have a similar effect. This concern is certainly debatable, but it is bolstered by the fact that the government is increasingly seeking assistance from technology companies to obtain data about users.[92]

[85] *See* Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1907 (2013).

[86] Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1188 (2012).

[87] *Id.* at 1215.

[88] 565 U.S. § 400 (2012).

[89] *Id.* at 402-03.

[90] *Id.* at 415 (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

[91] *Id.* at 416.

[92] *See* Ian Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873, 2875 (2018). It is worth noting that the government may have a more difficult time in getting this assistance, as the Supreme Court held (during the drafting of this essay) that prior to obtaining location data from cell phones, "the government generally must obtain a warrant supported by probable cause." Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018)

Lawmakers and regulators are aware of these concerns. The FTC, which has the responsibility to protect consumer data privacy in connection with autonomous vehicles, held an event focused entirely on the issue in June of 2017.[93] Also in 2017, Senator Edward Markey introduced a congressional bill that aimed "[t]o protect consumers from security and privacy threats to their motor vehicles, and for other purposes."[94] The Bill, titled the "Security and Privacy in Your Car Act of 2017" or the "SPY Car Act of 2017," provides that "[a] manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee."[95] It remains unclear, however, whether this bill would prevent wireless ISPs from gathering and sharing location data independently of the GPS sensor in a vehicle.

The auto industry is aware of the privacy concerns too. In an interview with Bloomberg, a vice president at GM commented, "[i]f consumers want to take advantage of these kinds of new connected features, especially making purchases while driving or using ride-hailing apps, they'll have to give up at least some privacy."[96] Interestingly, however, automakers have expressed concerns over passenger privacy when the government has considered safety rules that would require them to share data with each other. In recent public comments solicited by the NHSTA in connection with "V2V" data sharing, approximately 73% of automakers involved expressed privacy concerns in their comments.[97]

III. MOVING FORWARD

This essay has provided only a snapshot of the swirl of policy challenges tied to autonomous vehicle data. These challenges relate to improving public safety, facilitating commerce, promoting innovation, and ensuring privacy. Policymakers and commentators have tended to focus on each of these problems independently. The NHTSA, for instance, has observed the fact that data-sharing

[93] *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, FED. TRADE COMMISSION (June 28, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected [https://perma.cc/PAT7-85CE].

[94] Security and Privacy in Your Car Act, S. 680, 115th Cong. (2017).

[95] *Id.* at § 4.

[96] Gabrielle Coppola & David Welch, *The Car of the Future Will Sell Your Data*, BLOOMBERG BUSINESSWEEK (Feb. 20, 2015, 5:00 AM), https://www.bloomberg.com/news/articles/2018-02-20/the-car-of-the-future-will-sell-your-data?utm_content=tech&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social&cmpid%3D=socialflow-twitter-tech [https://perma.cc/N9T3-QSJW].

[97] Anne E. Boustead & Karlyn D. Stanley, *The Legal and Policy Road Ahead: An Analysis of Public Comments in NHTSA's Vehicle-to-Vehicle Advance Notice of Proposed Rulemaking*, 16 MINN. J.L. SCI. & TECH. 693, 716 (2015). For all comments submitted in response to the NHTSA's solicitation, see *Automated Driving Systems: A Vision for Safety*, REGULATIONS.GOV, https://www.regulations.gov/docket?D=NHTSA-2017-0082 [https://perma.cc/QU53-8YEV].

implicates privacy issues but says the issue falls under the FTC's authority. Scholars have been more willing to grapple with the interplay between these policy goals, but the relationships haven't been explored deeply yet. Scholars who have examined these policy issues in isolation have provided invaluable insights, however, and their work has laid the necessary foundations for this essay.

The policy issues raised by autonomous vehicle data cannot be solved in isolation. A new law mandating extensive data sharing to improve passenger safety, for instance, might encroach upon passenger privacy and dampen competition. By the same token, a law forbidding automakers from tracking the locations of vehicles would promote privacy at the expense of commerce and possibly safety. Only by deeply grappling with the relationships between safety, commerce, innovation, and privacy can we ask the new questions that will push policy ahead. The following questions, drawn from the foregoing analysis, are offered as starting points:

> ***Question 1: What is the minimal amount of vehicle data from which automakers can meaningfully improve safety?*** In a 2011 essay, technology and social media scholars Danah Boyd and Kate Crawford wrote, "Bigger Data are Not Always Better Data."[98] Their point was that, sometimes, useful things can be accomplished with less than all of the available data.[99] (Volume does not equate to usefulness.) Following on this insight, it would be helpful for policymakers to have a clearer sense of whether automakers could learn from one another without sharing their most commercially valuable data. According to the reports cited earlier in this piece, the most useful purpose of data-sharing among automakers would be to reveal "edge-cases"—scenarios that cars seldom encounter, and might be unable to handle without specific training. Might it be sufficient in some cases for automakers to merely be aware of the general nature of an edge case—e.g., the side of a white truck being mistaken by a vehicle for the sky—rather than having *all* of the data collected by a competitor? Sharing the underlying data from a vehicle might not always be a necessary step for industry-wide learning. In fact, the research presented earlier in this essay suggests that lawmakers and the public have often pushed automakers to share data not necessarily with one another, but with the public.[100] This push for public accountability following accidents has become somewhat conflated with the safety benefits that might come from data-sharing. If useful lessons can be drawn from generalized descriptions of edge-cases, then perhaps policymakers could promote safety without diminishing the value of trade secrets or passenger privacy.

[98] Danah Boyd and Kate Crawford, *Six Provocations of Big Data* 6 (presented at A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Sept. 21, 2011), http://ssrn.com/abstract=1926431.

[99] *See id.* at 8.

[100] *See supra* notes 38-39.

Question 2: Can ISPs play a part in improving safety? As mentioned earlier, in 2017, Comcast submitted a statement to the FCC arguing (a bit confusingly) that the repeal of network neutrality rules would allow telecommunications companies to tap new sources of revenue which could fund the deployment of faster wireless infrastructure. The comment implied that high speed wireless internet connections are necessary for autonomous vehicle safety. Technology commentators quickly criticized Comcast, as no planned uses of data for safety purposes would require high speed connections to the internet.[101] But perhaps ISPs could be required to make good on the idea. Imagine a future where vehicles automatically detect and document extremely dangerous behavior — the telltale violent swerving of a drunk driver, for instance. These vehicles might monitor only their own drivers' behavior, or that of other nearby cars on the road. Such a system would prompt new privacy concerns, of course, but could also help police departments across the nation focus their energies on protecting the public from public safety threats. Under a new legal framework, ISPs might be required to transmit such automatically-generated police reports across new highspeed infrastructure (at no extra fee to the sender). The benefits that such an automatic reporting system would offer might well be outweighed by the costs and concerns, however.

Question 3: How safe is safe enough (and when must that goal be met)? As mentioned earlier in this essay, mandatory sharing of data among automakers has the potential to improve highway safety in the short term, and also suggests a reduction in competition for safety-related inventions over the long term. This could result, in theory, in cars that are less safe in the long run than they would otherwise be under competitive conditions. This is not an argument *against* data-sharing, but rather conjecture regarding the potential costs to innovation. Policymakers, the public, and the auto industry may need to face an uncomfortable question: "How safe is safe enough?"[102] Autonomous vehicles are unlikely to entirely eliminate highway fatalities, but they appear to have the potential to significantly reduce them.[103] Are we willing to sacrifice long-term safety gains for smaller short-term improvements? By the same token, are we willing to accept more danger in the short-term for more long-term safety improvements that remain speculative?

Question 4: To what extent are automakers relying on trade secrecy rather than patent protection for their algorithms? The evidence presented

[101] *See supra* note 83 and accompanying text.

[102] Halsey, *supra* note 36.

[103] U.S. DEP'T OF TRANSP., DOT HS 812 442, AUTOMATED DRIVING SYSTEMS 2.0 A VISION OF SAFETY, at i (Sept. 2012), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf [https://perma.cc/MW4Y-3JGN] ("ADSs have the potential to significantly reduce highway fatalities by addressing the root cause of these tragic crashes").

in this essay suggests that some automakers are reluctant to share data because doing so could help competitors reverse-engineer algorithms maintained as trade secrets. If manufacturers more readily sought patent protection for these algorithms, they would be required to disclose those inventions to the public, removing a barrier that appears to be hindering data-sharing. The question would require deeper research to answer, and could be worth investigating. A hypothesis is that recent Supreme Court jurisprudence—most notably the Court's decision in *Alice Corp. v. CLS Bank Int'l*—has made trade secret protection a more attractive choice for protecting some types of algorithms that relate to autonomous vehicles.[104]

Question 5: What if the government required vehicle makers to demonstrate safety based upon a measure of total vehicle miles or hours? This idea is offered as both an open question and a possible solution that might help the industry and the public balance their interests. A rule requiring all automakers to clock a certain number of accident-free miles—say, five million miles across all vehicles in a fleet—under a probationary period could create new patterns of cooperation. A large automaker could meet the requirement in a short time by adding together the miles traveled by all of its cars. A smaller automaker with fewer vehicles to test could meet the requirement by joining forces with other small automakers to form a cooperative "fleet" that would be eligible to record a combined number of miles on the condition that each member of the fleet shares data with the other members even after the companies meet the mileage threshold—a data pool. Such a regime would allow for a degree of data-sharing to improve safety while leaving open the possibility that a large automaker could distinguish itself in the marketplace by assuring consumers greater privacy by promising not to share their data. This result aligns with an argument I have made elsewhere that "incomplete" or fragmented cooperation in some settings is economically and socially optimal.[105]

So many of the challenges related to autonomous vehicle data are about control. Automakers want control over this data to preserve a competitive edge. The automakers with the strongest incentive to do so are those that have the most to gain from collecting it, and those that have the most to lose from its widespread disclosure.[106] Wireless ISPs, meanwhile, will enjoy immense control over vehicle location data under the current legal and regulatory framework. Congress' repeal of the FTC's 2016 privacy rules allows ISPs to gather and repackage location data and other information that networks of advertisers are eager to buy.

[104] Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347 (2014).

[105] Michael Mattioli, *Patent Pool Outsiders*, 33 BERKELEY TECH. L. J. 225, 282-83 (2018).

[106] A 2017 article exploring the issue seems to capture the problem well: "Safety will be seen as a key competitive advantage for leaders in autonomous-vehicle technology, and giving up crash data has negative effects for both leaders and laggards. For leaders, it allows competitors to profit from their hard-won knowledge – and, potentially, to catch up. For laggards, it exposes vulnerabilities." Tillemann and McCormick, *supra* note 30.

The 2017 repeal of network neutrality rules, meanwhile, will allow ISPs to offer highly tailored data packages and advertising experiences based on location-tracking. These new forms of surveillance are helpful to advertisers and retailers, and strike a blow to privacy interests that American law has traditionally sought to defend.[107]

At the center of it all is the public. Accepting the very idea of an autonomous vehicle requires a willingness to give up control. But now we must consider how much control over our privacy and safety we are also willing to give up when we let computers take the wheel. Likewise, how much control will automakers give up in order to maximize safety? These questions can't be examined in isolation. Instead, we must understand the data itself, the interests of stakeholders who want to control it, and how the law governs that control. In this way, we might hope to resolve the most important question of all: will the public have a say in the driverless future, or will we all just be going along for the ride?

[107] *See* Glancy, *supra* note 86; *see also* Michael McGowan, *Driverless Cars: Safer Perhaps, But Professor Warns of Privacy Risks*, GUARDIAN (Sept. 21, 2017), https://www.theguardian.com/technology/2017/sep/22/driverless-cars-safer-perhaps-but-professor-warns-of-privacy-risks [https://perma.cc/Q6R6-D5E3].