YOUR PRIVACY ON THE ROAD: WHAT IS COLLECTED AND HOW IT IS UTILIZED

Melanie Reid*

TABLE OF CONTENTS

I. INTRODUCTION 35

II. DATA COLLECTED AND THE PRIVACY IMPLICATIONS 38
- A. SURVEILLANCE ON THE ROADS – CAMERAS, CAMERAS, AND MORE CAMERAS 39
  - *1. Existing Technology* 39
  - *2. Fourth Amendment Implications in the U.S.* 43
- B. DATA FOUND INSIDE THE CAR 47
  - *1. Existing Technology* 47
  - *2. Fourth Amendment Implications in the U.S.* 50
- C. DATA COLLECTED BY THE AUTONOMOUS VEHICLE COMPANY 54
  - *1. Existing Technology* 54
  - *2. Fourth Amendment Implications in the U.S.* 58

II. SURVEILLANCE CAR DATA'S IMPACT IN A LEVEL 3 WORLD VERSUS A LEVEL 5 WORLD 62
- A. EVIDENCE COLLECTED FROM AN AV AND PRESENTED TO A JURY WILL PAINT A MORE ACCURATE PICTURE OF WHAT OCCURRED AT THE TIME OF THE CRASH. 67
- B. HUMANS MAY STILL BE HELD CRIMINALLY LIABLE IN LEVEL 3 CONDITIONAL AUTOMATION AND EVEN IN A LEVEL 5 FULLY AUTOMATED DRIVING WORLD. 68
- C. EXPECT MORE TRAFFIC ACCIDENTS AND CRIMINAL PROSECUTIONS IN A LEVEL 3 CONDITIONALLY AUTOMATED WORLD AS HUMAN DRIVERS BECOME MORE COMPLACENT AS AV SYSTEMS TAKE OVER MOST OF THE DRIVING. 69
- D. SOCIETY (AND LEGISLATURES) MUST DECIDE WHETHER ENFORCEMENT OF TRAFFIC LAWS IS NECESSARY

* Professor of Law, Lincoln Memorial University-Duncan School of Law. I would like to thank Stefanie Bowen and Evan Pease for their invaluable research assistance and Adam Gershowitz, Brian Owsley, and Zachary Kaufman for their comments and feedback. I would also like to thank the SEALS Criminal Procedure discussion group members for their support and advice.

(AND ADVANTAGEOUS) AS WE ADVANCE FROM A LEVEL 3 TO A LEVEL 5 FULLY AUTOMATED DRIVING WORLD 73

IV. CONCLUSION 74

I. INTRODUCTION

When you go for a quiet ride on the open road, how much privacy do you have? The answer is a lot less than you think. Consider these three scenarios:

Scenario 1: Surveillance cameras on public roadways

Driver X is late for work. She grabs her coffee and toasted bagel and jumps in the car. Her smart phone sends her an alert that it will take approximately forty-five minutes to get to work today. She needs to hurry. As she is driving, she fiddles with the Apple CarPlay system and chooses to play the podcast she was listening to earlier that morning. A red-light camera takes a picture of her and her car at that moment as she drives through a yellow-turning-red light at a busy intersection. She will receive the traffic violation in the mail a week later. Unaware her picture was just taken; she then asks the GPS in her car to find the quickest route to work and settles in to eat her bagel and drink her coffee. The traffic seems heavier than normal, so she decides to take a toll road (even though she left her E-Z pass transponder in her husband's car). Cameras and antennas are suspended above the toll road to collect the fees electronically. The toll road cameras take photos of the front and back of Driver X's car, and sensors in the ground follow her car as she changes lanes. The sensors in the road know whether the passing vehicle has more than two axles so they can charge the appropriate toll rate. Computers then search for a license plate that matches Driver X's license plate. Driver X, the registered owner, will now receive a second bill in the mail for using the toll road without paying.[1] She then enters the highway and puts the car in cruise control. A drone flying above clocks her speed as faster than the speed limit and sends her a speeding ticket. This is her third traffic surveillance encounter of the day and it's only been twenty minutes.

Scenario 2: A vehicle's Event Data Recorder (EDR)

Driver Y has three previous DUIs (driving while intoxicated), and his

[1] Such equipment even contains color and infrared technology that is used to penetrate license plate shields that are meant to thwart toll cameras. Dave Forster, *Get a Peak at Toll-Road Technology*, GOV. TECH. (Jan. 31, 2014), https://www.govtech.com/transportation/get-a-peek-at-toll-road-technology.html.

license has been revoked. Despite having his license revoked, he chooses to go to several bars that night and drink and then drive his beloved Tesla Model 3. Driver Y enters the highway and enables Autopilot, the car's advanced driver assistance system. A police officer pulls out of the median and drives behind the Tesla on the highway. An automated license plate reader (ALPR) that is attached to the police squad car captures all license plate numbers that come into view along with the location, date, and time. The data, which includes photographs of the Tesla and the driver, is uploaded to a central server. The system sends an alert to the officer in the squad car to let him know the registered owner of the Tesla has had his license revoked. The police officer turns on his lights, and Driver Y begins to speed. At the next curve, the Tesla swerves and hits a light pole. Driver Y is arrested for driving while his license is revoked, and the police officer then proceeds to retrieve the car's event data recorder (EDR). The EDR tracked the vehicle's speed, acceleration, braking, steering, and air-bag deployment before, during, and after the crash. The police use this information to convict Driver Y of reckless driving and another DUI.

Scenario 3: The information collected by car manufacturers

Driver Z is pulled over for speeding. The police officer sees several suitcases in the backseat. He asks Driver Z where she is going, and she gives conflicting answers. She appears "very nervous" when speaking to the police officer as she rubs her face and is breathing very hard and fast. The police officer suspects she is not telling the truth, and in his experience working in interdiction, believes she is driving to "a destination city for contraband."[2] Driver Z gives the police officer consent to search the car, and he finds five large gallon size Ziploc bags containing a large amount of U.S. currency in one of the suitcases. The police officer seizes the money and the vehicle and detains Driver Z on suspicion of being involved in criminal activity. The police officer later subpoenas the car manufacturer and learns the car's physical location for the last thirty days, when the car was being driven, who was driving the car based on voice commands given inside the car, and what was happening inside the car as data was being collected from the car's radar sensors and cameras. This information gives the police enough information to build a money laundering case against Driver Z.

The use of electronic surveillance on our roads and in our vehicles has a considerable impact on criminal procedure in the United States and beyond. Our cars collect a lot of information on us – where and when we go places, what we like to listen to, what we like to do and say inside our cars, and even how attentive we are when we are driving. And when we use a car manufacturer's app to monitor where our child or spouse is on the road to

[2] *See* Uhunmwangho v. State, No. 09-19-00119-CR, 2020 WL 1442640, at *1–4 (Tex. App. Mar. 25, 2020) (serving as the basis for this factual scenario).

time dinner perfectly, our car manufacturers are collecting this data as well.

These methods of data collection during criminal investigations will soon become routine as vehicles move from partially to fully automated and surveillance is conducted both outside and inside the car. The cars manufactured today collect and in the future will collect a lot of data. Because of this massive data collection, these cars with their own artificial intelligence have become incredibly "smart" and will become even "smarter" as they learn from real-life experience and in simulations. Cars have evolved from having no automation (designated as Level 0 on the Society of Automotive Engineers (SAE) automation level) to partial automation (Level 2) where a vehicle has combined automated functions, like acceleration and steering, to full automation (Level 5) where a vehicle is capable of performing all driving functions under all conditions and the driver has the option to control the vehicle.[3] Most autonomous vehicles private individuals can purchase are currently at Level 2 which still requires a physically present driver to be in the driver's seat and capable of operating the vehicle. There are a few Level 3 vehicles, like the Audi 8 or the BMW iNext, that the public can purchase, but even at a Level 3, a driver must be ready to take control of the vehicle at all times with notice.[4] Fleet cars, such as Lyft or Uber, or trucking fleets[5] will more than likely be the first to have access to Level 5 full automation vehicles as Automated Driving Systems (ADS) is incredibly expensive, and it will take several test runs/pilot programs and "life experiences" before the artificial intelligence in the car is ready and capable of being fully autonomous.

Some scholars have written on the impact autonomous vehicles (AV) will have on criminal law and procedure.[6] But the question remains, how will

---

[3] SOC'Y OF AUTO. ENG'RS (SAE), *J3016 Levels of Driving Automation* (May 3, 2021), https://www.sae.org/binaries/content/assets/cm/content/blog/sae-j3016-visual-chart_5.3.21.pdf [hereinafter SAE].

[4] *See generally The Future of Driving is Autonomous,* BMW GROUP, https://www.bmwgroup.com/en/innovation/technologies-and-mobility/autonomes-fahren.html (last visited Feb. 19, 2022).

[5] Marco della Cava, *Self-driving Truck Makes First Trip—a 120-mile Beer* Run, USA TODAY (Oct. 25, 2016), https://www.usatoday.com/story/tech/news/2016/10/25/120-mile-beer-run-made-self-driving-truck/92695580/.

[6] *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1208 (2012); Jordan Blair Woods, *Autonomous Vehicles and Police De-Escalation*, 114 N.W. U.L. REV. ONLINE 74, 74 (2014) (arguing that autonomous vehicles will decrease possibilities for escalation during vehicle stops); Jeffrey K. Gurney, *Crashing into the Unknown: An Examination of Crash-Optimization Algorithms Through the Two Lanes of Ethics and Law*, 79 ALB. L. REV. 183, 205 (2016); Lindsey Barrett, *Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception*, 106 GEO. F. J. 181, 197–203 (2017); Leesa Guarnotta, *Death of the Dui: Should Autonomous Vehicles Be Considered Synonymous to Designated Drivers Under Georgia Law?*, 70 MERCER L. REV. 1113, 1126

the United States adjust to the Autonomous Age and this new frontier of digital information? Surveillance and tracking tools such as GPS devices, license plate readers, traffic light cameras, and vehicle radar, Light Detection and Ranging (LIDAR), audio, and video recording devices and surveillance systems, are much more intrusive, revealing, detailed, and comprehensive than ever before. The government has access to where travelers are going, who is in the car, what they are doing in the car, at what speed they are traveling, and at what time of the day they chose to travel. Cars now contain their own artificial intelligence systems in their hardware and software, sensors, cameras, radars, etc. Part II of this article will evaluate the amount of evidence readily available for the government to collect in preparation for criminal prosecutions and ask whether the third-party doctrine or other Fourth Amendment doctrine applies to such information. Similarly, Part III of this article will explore the car data's impact in Level 3 conditional automation compared to Level 5 full automation. Evidence collected from AVs and presented to a jury will paint a more accurate picture of what occurred at the time of the crash. Most of this data is incredibly "detailed, encyclopedic, and effortlessly compiled," and therefore warrants should be required to access this data. Human beings will still be held criminally liable in a Level 3 driving world and quite possibly, even in a Level 5 fully automated world. Lastly, society must re-examine whether we want to continue enforcing strict liability traffic laws as we evolve from a Level 3 to a Level 5 driving world. This paper seeks to explore such criminal law and criminal procedure consequences in the Autonomous Age.

II. DATA COLLECTED AND THE PRIVACY IMPLICATIONS

While some may choose to drive a 1980s Chevy to avoid the travel diary (aka event data recorder or EDR) placed in recently made cars or the artificial intelligence in ADS collecting data and transmitting it to the AV company, those old-school drivers will still have to accept the reality that the government is collecting and monitoring our travel on public roads daily. Combined with other forms of collected data, such as cell phone location information, phone conversations, or apps we may be using while driving, the government will have a pretty easy time backtracking our movements on the day a crime or traffic violation is committed. The data collected and to later be analyzed (either proactively to stop a crime in progress or reactively

(2019); Jeffrey K. Gurney, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles,* 5 WAKE FOREST J.L. & POL'Y 393, 410–29 (2015); Callie A. Kanthack, *Autonomous Vehicles and Driving Under the Influence: Examining the Ambiguity Surrounding Modern Laws Applied to Future Technology*, 53 CREIGHTON L. REV. 397, 421 (2020); and Nanci K. Carr, *As the Role of the Driver Changes with Autonomous Vehicle Technology, So, Too, Must the Law Change*, 51 ST. MARY'S L.J. 811, 812 (2020).

to solve a crime already committed) can be divided into three categories: (a) government-owned surveillance systems, (b) data obtained from inside the car (the EDR), and (c) data obtained from the car company itself.

A. Surveillance on the Roads – Cameras, Cameras, and More Cameras

1. Existing Technology

Closed-circuit television (CCTV) or video surveillance is commonplace. CCTV can be found in public places such as shopping centers, banks, and parking lots, and many private citizens and homeowners choose to install CCTV on their own property. The Ring app has made it incredibly easy for homeowners to place cameras throughout their property and wait for alerts when the motion detection sensor is set off to identify and talk to the person who is at the door.[7]

Our public roadways are equally monitored. Many cities have red-light enforcement programs and "SmartWay" traffic cameras.[8] Live web cams are posted at various locations along public highways and roads, presumably so that travelers can "locate construction areas, view message signs, and find out about road conditions."[9] The video footage can be seen in real-time, and while most of the cameras do not identify the driver, the cameras get a clear view of the make and model of each car passing by. The red-light cameras mounted on red lights and stop signs take a picture of every car that appears to run a red light. Many traffic cameras use a camera and radar device to simultaneously take a photo of the vehicle and to measure the

---

[7] *See The Security Camera Buyer's Guide*, RING DOORBELL, https://support.ring.com/hc/en-us/articles/360041531472-The-Security-Camera-Buyer-s-Guide (last accessed Feb. 26, 2022). In fact, my neighbor recently told me that he had placed a camera in his yard so that he knows every time people pass by his home, and he is familiar with the neighbors' daily travel schedules.

[8] *Automated Enforcement Overview*, NATIONAL CONFERENCE OF STATE LEGISLATURES, (July 21, 2020), https://www.ncsl.org/research/transportation/automated-enforcement-overview.aspx#:~:text=Currently%2C%20city%20and%20local%20governments,of%20Columbia%20use%20red%2Dlight ("Nearly 350 U.S. communities use red-light cameras, and more than 150 communities use cameras to enforce speed laws.").

[9] CITY OF KNOXVILLE SMARTWAY TRAFFIC CAMERA PORTAL, https://knoxvilletn.gov/residents/streets_traffic_transit/tdot_smart_way_traffic_cameras (last accessed Feb. 26, 2022). There are also traffic data collectors which record the amount of traffic through a particular area. They track the amount of traffic, the time of day, and the weather. This information would prove to be helpful if the traffic data collector was placed on a dead-end street with one house that the government wished to surveil. Perhaps it could be used to monitor the number of visitors to a suspected drug dealer's home?

vehicle's speed.[10] Toll road systems such as EZPass use similar camera systems.[11] The use of all of these cameras is regulated by various state laws,[12] and many states rely on a population-based algorithm that considers the number of intersections to determine how many automated ticketing cameras a town may have.[13] Many drivers appear to dislike the idea of being issued automated tickets for speeding or running red lights. Tennessee State Representative Andy Holt filmed himself burning an automated ticket and urged his constituents not to pay their red-light camera enforcement tickets.[14] He argued that because it is a civil citation and not a criminal citation, it is unnecessary to pay them as most of the money goes to the red-light traffic camera company that manufactures and monitors the cameras.[15]

Human police officers are no longer needed to issue a speeding ticket. Speed cameras, also known as photo radar or automated speed enforcement, record a vehicle's speed using radar and take a photograph of the vehicle when it exceeds the speed limit.[16] Speed cameras have been known to be used

---

[10] Jonathon Bates & Shelly Oren, *Enforcing Traffic Laws with Red-Light and Speed Cameras*, 28 LEGISBRIEF 1, 1 (2020).

[11] *Criminal Justice Standards: Law Enforcement Access to Third Party Records*, ABA-CRIMINAL JUSTICE SECTION, (2013), https://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/.

[12] *See State Laws: Speed and Redlight Cameras*, GOVERNOR'S HIGHWAY SAFETY ASS'N, https://www.ghsa.org/state-laws/issues/speed%20and%20red%20light%20cameras (last accessed Mar. 6, 2022) (listing each state's regulations).

[13] Therefore, municipalities with lesser populations may be subject to fewer traffic cameras compared to bigger cities. A larger population size can lead to a greater presence of technology as much of this traffic technology is available to police on a funding-based basis. Precincts with a smaller population size may not have the budget to afford the latest technology tools. For example, Big Stone Gap, Virginia (population of 5,257) has a police/fire budget of $1,468,800 versus Richmond, Virginia (population of 226,622) has a public safety budget of $197,457,297.

[14] Jeni Diprizio, *Verify: Do You Really Have to Pay The Fine for a Red-light Ticket in the Mid-South?,* LOCAL24 MEMPHIS (Feb. 9, 2020), https://www.localmemphis.com/article/news/local/verify-do-you-really-have-to-pay-the-fine-for-a-red-light-ticket-in-the-mid-south/522-8e069bb1-1c96-401c-98fa-cf18cb38c51a. (According to Holt, "If you look on those citations—if they are run according to the law here in the state of Tennessee—it clearly says 'non-payment of this citation cannot adversely affect your credit report or credit score, your driver's license points, or your automobile insurance rates.' . . . You'll receive letters. You'll receive baseless threats. You'll receive collection notices. You'll receive letters from attorneys. All those things are intimidation tactics.").

[15] *Id.* There has been a backlash against red light cameras such that some jurisdictions no longer use them. *See* Corey Dade, *What's Driving the Backlash Against Traffic Cameras?*, NPR (Feb. 22, 2012), https://www.npr.org/2012/02/22/147213437/whats-driving-the-backlash-against-traffic-cameras (discussing the "outrage coming from hundreds of communities using red-light and speed cameras").

[16] *Motor Vehicle Safety: Automated Speed-Camera Enforcement*, CENTERS FOR DISEASE CONTROL AND PREVENTION,,

in 12 states and the District of Columbia.[17] As Ford recently filed a patent for a self-driving police car, perhaps we might see more speeding tickets being issued by cameras and machines rather than humans.[18]

One of the most effective ways to surveil the public roadways is through ALPRs. Active ALPRs can record all license plates that come into their view, while also noting the location, date, and time. Police mount them to police cars or objects like road signs, poles, and bridges and take pictures of license plates as they pass by.[19] If the system scans a car on the list, the police officer is given an alert. Over time, the data can expose a car's historical travel. Using an algorithm applied to the data, the system can uncover regular travel patterns and predict the driver's future movements.[20] The data can also disclose all vehicles in a particular location at a particular time.[21] In addition to capturing license plate data, the photographs can reveal images of the vehicle, the vehicle's driver and passengers, as well as its immediate surroundings—and even people getting in and out of a vehicle.[22]

The use of ALPR is widespread among law enforcement agencies. "According to a 2012 report by the Police Executive Research Forum, approximately 71% of all U.S. police departments use some type of ALPR system."[23] ALPR is used to recover stolen vehicles, to identify wanted felons,

---

https://www.cdc.gov/motorvehiclesafety/calculator/factsheet/speed.html (last accessed Mar. 6, 2022).

[17] *Id.* ("The first automated speed limit-enforcement program actually began in Paradise Valley, Arizona in 1987. . . . Since then, at least 92 jurisdictions (state and local) have adopted automatic enforcement, although speed cameras are not as widely used as red-light cameras.").

[18] U.S. Patent Application No. 2018/0018869 A1 (issued Jan. 18, 2018); Peter Holley, *For Wants to Patent a Driverless Police Car that Ambushes Lawbreakers using Artificial Intelligence,* WASH. POST (Jan. 31, 2018), https://www.washingtonpost.com/news/innovations/wp/2018/01/30/ford-submitted-a-patent-for-an-autonomous-police-car-the-u-s-government-just-approved-it/ ("A police autonomous vehicle would use its radar and lidar systems to determine "the patrol car speed along with whether a targeted vehicle is approaching or departing in relation to the radar/lidar unit in order to accurately determine a vehicle's speed. . . . Vehicles equipped with forward and rearward facing systems may monitor vehicle speed from all directions, stationary or while moving.").

[19] *See* Theophilus O. Agbi*, Hands Off My License Plate: The Case for Why The Fourth Amendment Protects License Plates From Random Police Searches,* 45 VT. L. REV. 125, 128–29 (2020) (discussing ALPR capabilities).

[20] *See* Kimberly J. Winbush, Annotation, *Use of License Plate Readers*, 32 A.L.R.7th Art. 8 § 2 (2017) (discussing police compiling data from ALPR to track a vehicle's locations).

[21] *Id.*

[22] *Id.*

[23] POLICE EXEC. RSCH. F., CRITICAL ISSUES IN POLICING SERIES: "HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING?" 1 (2012).

missing persons, parolees, sex offenders, illegal aliens, gang members, or suspected terrorists, to collect revenue from individuals who are delinquent on city or state taxes or fines, and to monitor "Amber Alerts."[24] While the ALPR system can process license plate numbers in real-time, the system can also collect and indefinitely store data from each license plate capture. These captured plate numbers can assist law enforcement later when investigating possible suspects of past crimes.[25] Laws vary among states as to the collection and retention of license plate information.[26]

ALPR is also being used to assist in parking enforcement. Automated traffic and parking enforcement software uses ALPR technology and artificial intelligence to track, record, and manage parking violations.[27] Police need no longer worry about chalking a vehicle to monitor the amount of time a car is parked in a particular spot. ALPR technology can capture license plates, evaluate how long a car is parked, and then electronically send the parking ticket to the car's owner.[28] ALPR technology can be used by officers using a handheld device or static cameras can be installed to assist with virtual vehicle chalking and tracking. The system is constantly learning by using past data "to improve data reads and validations."[29]

In summary, government and private-owned cameras are currently watching a driver's every move on public and private roads and in parking lots. And it's very possible that in the future, autonomous police vehicles could issue tickets without needing to ask drivers to pull over.[30] The

---

[24] The Department of Homeland Security proposed a federal database to combine all monitoring systems, which was later canceled after privacy complaints. Ellen Nakashima & Josh Hicks, *Department of Homeland Security Cancels National License-plate Tracking Plan*, WASH. POST (Feb. 19, 2014), https://www.washingtonpost.com/world/national-security/dhs-cancels-national-license-plate-tracking-plan/2014/02/19/a4c3ef2e-99b4-11e3-b931-0204122c514b_story.html.

[25] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 330 (2015).

[26] As of February 2022, 16 states have limits on how long the data may be retained, with the shortest being New Hampshire (3 minutes) and longest Colorado (3 years). *Automated License Plate Readers: State Statutes*, NAT'L CONF. OF STATE LEG. (Feb. 3, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx.

[27] *About License Plate Recognition (LPR) Parking Enforcement*, PASSPORT OPERATING SYSTEM (Jan. 6, 2020), https://www.passportinc.com/blog/about-license-plate-recognition-lpr-parking-enforcement/.

[28] *Id.*

[29] *See Parking Enforcement with ViolationAdmin*, OMS-COM, https://ops-com.com/parking-security-platform/parking-enforcement/ (last visited Feb. 19, 2022) (demonstrating how past data is used to reduce future errors when tracking vehicles and reading the license plate numbers correctly).

[30] Peter Holley, *Ford Wants to Patent a Driverless Police Car that Ambushes Lawbreakers Using Artificial* Intelligence, WASH. POST (Jan. 31, 2018),

technology that is already available, ALPR, surveillance cameras, lasers, radar, and roadside sensors, and real-time access to government records will allow police AVs to identify and follow speeding vehicles or those who run red lights or fail to stop at stop signs. The police AV, according to Ford's patent, would be able to communicate with a remote central computing system to verify the legal speed for a given section of the road and then communicate with the offending vehicle and ask if it is driving autonomously or by a human operator and ask if it might provide a driver's license.[31] Tickets would be issued remotely, and a record of the incident would be sent to the police station or the department of motor vehicles.[32] Now, more than ever, highway travel is heavily monitored and scrutinized.

2. Fourth Amendment Implications in the U.S.

How has the U.S. Supreme Court handled government surveillance in public areas? The Supreme Court has been consistent in past cases like *Knotts* and *Karo* in stating that the government can monitor a person's travel on public roads (using tracking devices, cameras, or otherwise) without the need for a warrant or any type of court order.[33] Therefore, surveillance done in public areas is outside any Fourth Amendment protections (as long as the police do not need to touch a person's "effect" and essentially commit a trespass in order to collect information).[34] "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[35] Anyone can observe a person's public movements and follow someone on public roads. And because the information could have been obtained from visual surveillance conducted by a human law enforcement agent, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and

---

https://www.washingtonpost.com/news/innovations/wp/2018/01/30/ford-submitted-a-patent-for-an-autonomous-police-car-the-u-s-government-just-approved-it/.

[31] *Id*.

[32] *Id*.

[33] United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

[34] United States v. Jones, 565 U.S. 400 (2012). None of the surveillance tools discussed above actually require a trespass on a person's effect, and therefore, it is not necessary to conduct a Jones trespass analysis. However, Justice Gorsuch argued that there could be a trespass in *Carpenter* even though there was no physical touching of the cell site location information. Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J. dissenting).

[35] *Knotts*, 460 U.S. at 280. *See generally* ANDREW FERGUSON, THE RISE OF BIG DATA POLICING (2017).

technology afforded them in this case."[36] *Knotts* and *Karo* were decided in the 1980s when law enforcement agents' sensory faculties were enhanced by placing large tracking device boxes on their laps in their car to assist them in keeping track of vehicles they were currently following. The Supreme Court may have had a hard time imagining cameras at every highway exit, ALPR systems, and self-driving police cars with all the camera bells and whistles. Despite significant advances in surveillance technology, *Knotts'* and *Karo's* impact has withstood the test of time (so far). Can the government continue to monitor the movements of citizens of public roadways as long as it is hypothetically conceivable to obtain information in a technologically enhanced manner from a lawful vantage point?

Another rationale the Supreme Court has provided to limit the amount of privacy we might have while traveling on public roadways is the fact that highways are highly regulated. Travelers have a reduced expectation of privacy due to the pervasive regulation of vehicles capable of traveling on public highways and the government's compelling need to ensure driver and passenger safety.[37] This (and the fact that a vehicle is extremely mobile) was the rationale given to justify why police do not need a warrant to search a vehicle.[38] Police only need probable cause to believe that contraband or evidence of a crime will be found in the vehicle before they can search.[39]

How did our founding fathers feel about government surveillance in public? It seemed to be the entry into private areas and the search of containers in our homes that bothered them most.[40] There is no indication that our founding fathers felt ill at ease if a customs officer passed them on a public street and observed what they were publicly doing.

The Supreme Court "has to date not deviated from the understanding that mere visual observation does not constitute a search."[41] Justice Scalia in the majority opinion in *Jones* refused to address whether visual observation through electronic means is an unconstitutional invasion of privacy but rather chose to decide the case by pointing out the law enforcement agent had to attach a tracking device to the defendant's vehicle to monitor his whereabouts, and this action, absent a warrant, constitutes a trespass and Fourth Amendment violation.[42]

---

[36] *Knotts*, 460 U.S. at 282.

[37] California v. Carney, 471 U.S. 386, 392 (1985).

[38] Carroll v. United States, 267 U.S. 132 (1925) ("A warrant is not needed to search the car—it is "not practicable to secure a warrant because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought.").

[39] *Carney*, 471 U.S. at 392.

[40] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[41] United States v. Jones, 565 U.S. 400, 412 (2012) (citing Kyllo v. United States, 533 U.S. 27 (2001)).

[42] *Id*. at 407 (citing *Knotts,* 460 U.S. at 286). "When the Government does engage in

In an age where a multitude of cameras are owned by both private individuals and government entities on practically every street corner, have our societal privacy expectations changed?

Justice Sotomayor would argue such monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[43] She asks, "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[44]

Justice Alito in his concurrence points out that many may find new technology that monitors your movements as "inevitable"—we sacrifice our privacy for increased convenience or security.[45] Long-term monitoring is conducted "relatively easy and cheap."[46] Justice Alito summarized his beliefs on government surveillance this way, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[47] While he failed to mention what is the cut-off between short-term and long-term monitoring, he believed "the line was surely crossed before the 4-week mark."[48]

Based on Supreme Court precedent in *Knotts*, dicta in *Jones*, and what society deems as reasonable as individuals install more and more cameras in their homes and on their roads, what should be required from law enforcement before they are given access to camera footage throughout town? It would seem if we follow Justice Alito's thinking, an officer investigating a crime that occurred on a particular day (i.e., a hit-and-run, an automobile accident where the driver may have criminal liability, a traffic violation, a crime that occurred in one day) should be able to access camera footage without a subpoena, court order, or search warrant. An officer investigating someone possibly involved in a conspiracy or crime that might cause significant planning over several months or years should need a search warrant signed by a judge to access several days, weeks, months, and even years of footage. The longer the monitoring (even though it may be done only in public areas), the more the government will learn intimate, personal

---

physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment."

[43] *Id.* at 415 (Sotomayor, J., concurring).

[44] *Id*.

[45] *Id*.

[46] *Id*. at 416.

[47] *Id*. at 430.

[48] *Id*.

information about an individual's daily routine, where they work, when they work or run errands, who they see, etc.[49] Drawing the line between short-term monitoring without a judicial check and long-term monitoring with a judicial check before receiving access to vast amounts of data seems sensible and takes into account the different privacy implications associated with the level of intrusiveness of long-term versus short-term monitoring.

What constitutes long-term monitoring? The Supreme Court in *Carpenter* took exception to two court orders, one seeking 152 days of cell-site records from MetroPCS and one seeking seven days of cell-site location information from Sprint.[50] The government did not apply for a warrant to access such data but rather they asserted to the magistrate judge that such records were "relevant and material to an ongoing criminal investigation" under the Stored Communications Act.[51] The Court found that the ease in which the government was able to obtain "12,898 location points cataloging Carpenter's movements" was unacceptable.[52] The location data's "deeply revealing nature" and "the inescapable and automatic nature of its collection" requires law enforcement to seek a warrant and gather probable cause before accessing such comprehensive data.[53] Therefore, we can surmise that the government may be able to request surveillance footage under the seven day threshold without obtaining a warrant. If the government wants to follow an individual using surveillance cameras for more than seven days, they need a warrant to do so.

On the other hand, the Court in *Carpenter* clarifies that their decision on cell site location information was "a narrow one"—"We do not call into question conventional surveillance techniques and tools, such as security cameras."[54] Is there a public camera surveillance exception? Will long-term monitoring via traffic cameras, ALPRs, red light enforcement cameras, toll road cameras, and CCTV withstand scrutiny after *Carpenter*?

The Fourth Circuit on a rehearing *en banc* recently reviewed the Baltimore Police Department's aerial surveillance program (AIR) in which

---

[49] *Id*. at 412. "There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is 'surely' too long and why a drug-trafficking conspiracy involving substantial amounts of case and narcotics is not an 'extraordinary offense' which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?" It makes much more sense to draw the line between short-term (single day) and long-term (multiple days) monitoring to require a warrant than choosing which crimes requiring long-term monitoring would require a warrant.

[50] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[51] *Id*. at 2210.

[52] *Id*. at 2212.

[53] *Id*. at 2223.

[54] *Id*. at 2220.

multiple planes fly around Baltimore "at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day, weather permitting," and the planes' cameras "capture roughly 32 square miles per image per second."[55] These images "can be magnified to a point where people and cars are individually visible, but only as blurred dots or blobs."[56] In the majority opinion, the Chief Judge stated that such "prolonged" surveillance "transcends mere augmentation of ordinary police capabilities."[57] "People understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time. But capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity."[58]

Have the amount of cameras on the road reached the level of pervasive and prolonged location monitoring similar to the monitoring conducted in the AIR program? Perhaps so, considering the thousands of cameras posted throughout many cities. The answer as to whether a warrant is necessary to access such footage may depend on the amount of data law enforcement is requesting to review. One day's worth of surveillance video to review what transpired before, during, or after a traffic accident may not require a warrant, while seven days' worth to conduct a large-scale criminal investigation may. Emergency short-term monitoring (i.e., Amber Alerts, hit-and-run suspects, etc.) would perhaps fit under the exigent circumstances exception to the warrant requirement. Courts are consistently attempting to reconcile Fourth Amendment case law with the ever-changing dynamics of more and more pervasive and prolonged surveillance tools. With the plethora of surveillance cameras and tracking tools available to both the government and the public, courts will repeatedly have to decide whether to narrow or broaden constitutional protections.[59]

B. Data Found Inside the Car

1. Existing Technology

Not only can law enforcement gather information concerning a vehicle's external activities while on public roads, but they can also access

---

[55] Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021).

[56] *Id.* at 334.

[57] *Id.* at 345.

[58] *Id.*

[59] *See* Laura Hecht-Felella, *The Fourth Amendment in the Digital Age: The Supreme Court's Carpenter Ruling Can Shape Privacy Protections for New Technologies*, BRENNAN CENTER FOR JUSTICE (Mar. 18, 2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age.

data collected inside the vehicle. A vehicle's electronic control module can store its location information, its traveling speed, what devices are connected to the vehicle, and what text messages, outgoing calls, and voice activation recordings are made in the car.[60] A vehicle system forensics tool used by investigators can extract this data from the vehicle to determine the history of the vehicle's whereabouts, what happened, and what the occupants were doing in the vehicle at the time of the crash.[61] Police can also use speedometer data gathered from a vehicle to enhance criminal penalties against a driver.[62] Investigators can also learn vast amounts of information collected in a vehicle's event data recorder (EDR).

On February 23, 2021, Tiger Woods was driving a Genesis GV80 luxury SUV down a hill near Los Angeles when his car hit the center median, then a curb on the other side of the road, and then a tree before flipping multiple times and settling in brush.[63] Police later accessed the event data recorder (EDR or black box) and learned that he was driving 84 to 87 miles per hour when he lost control of the vehicle (the speed limit was 45), and at that time, the EDR indicated he was pressing the accelerator instead of the brake.[64] The Los Angeles County Sheriff's Lomita Station Captain stated that "[t]he primary cause was driving at a speed unsafe for the road conditions and an inability to negotiate the curve of the roadway . . . [I]t's believed that when you panic or you have some sort of sudden interruption when you're driving, your initial thought is to hit the brake. It's believed that he may have done that—but hit the accelerator and didn't hit the brake."[65] Despite learning that he was speeding, police did not issue Woods a citation because there were no witnesses, and they did not want to base a citation on the EDR data.[66]

The EDR typically records the few seconds before, during, and after a crash. The typical data an investigator would find on an EDR[67] is: "(1) the

---

[60] Olivia Solon, *Insecure Wheels: Police Turn to Car Data to Destroy Suspects' Alibis*, NBC NEWS (Dec. 28, 2020), https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939 [hereinafter *Insecure Wheels*]; *see also* BERLA, https://berla.co/discover/) (Berla is a company offering a product to be used by law enforcement for vehicle systems forensics.

[61] *Insecure Wheels*, *supra* note 60; *see also* BERLA, *supra* note 60.

[62] *See* Brief for the ACLU as Amicus Curiae Supporting Appellant at 6, Mobley v. State, 834 S.E.2d 785 (2019) (No. S18G1546) (listing a number of relevant sources regarding vehicles and the information stored inside of them).

[63] Andrew Beaton, *Tiger Woods's Car Accident Was Caused by Unsafe Speeding*, THE WALL STREET JOURNAL (Apr. 7, 2021 1:34 pm ET), https://www.wsj.com/articles/tiger-woods-update-crash-cause-investigation-speeding-injuries-11617816842.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] 49 CFR § 563.5 ; *see also* John Day, *Tiger Woods Accident and 'Black Box' Data*, TENNESSEE INJURY LAW CENTER (Apr. 9, 2021),

driver's inputs—things like steering, braking, etc.; (2) seatbelt usage and airbag deployment information; (3) the status of the vehicle's systems before the crash; (4) pre-crash vehicle dynamics; (5) the severity of the crash; and, (6) whether the automatic collision notification performed."[68] Investigators need to immediately retrieve the EDR and not allow for the ignition to be turned on after the accident, or else the data, which is recorded in a continuous loop, may be erased.[69] An estimated 96% of all new cars come with an EDR installed, and almost every major automaker selling cars in the United States builds EDRs into new vehicles.[70]

The National Highway and Transportation Safety Administration (NHTSA)[71] attempted to enact a rule in 2014 requiring EDRs to be installed in all new vehicles and make EDR data publicly available. [72] However, the NHTSA abandoned the mandate in 2019 since most car makers began to voluntarily install "black boxes" on new vehicles.[73] Fifteen states have EDR-specific statutes that generally restrict access to the EDR or limit the use of recovered information.[74] The Driver Privacy Act of 2015 states that for an investigator to access the EDR data, he/she would need to (1) obtain the consent of the vehicle owner (or lessee) or (2) be authorized by a court or judicial or administrative authority, subject to the standards for admission into evidence, or (3) be carrying out investigations or inspections authorized by federal law, or (4) be conducting traffic safety research, so long as the personal information of the owner/lessee is not disclosed.[75]

---

https://www.tennesseeinjurylawcenter.com/tiger-woods-accident-and-black-box-data/ ("After a certain number of ignition cycles, the data is erased.").

[68] Day, *supra* note 67; *see also* Michelle V. Rafter*, Decoding What's in Your Car's Black Box: Who Owns the Data and Who Can Tap It?,* EDMUNDS (Jul. 22, 2014), https://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html ("Based on a separate NHTSA regulation passed in 2012, if a vehicle today does have an event data recorder, it must track 15 specific data points, including speed, steering, braking, acceleration, seatbelt use, and in the event of a crash, force of impact and whether airbags deployed.").

[69] Day, *supra* note 67.

[70] Rafter, *supra* note 68.

[71] The NHTSA establishes safety regulations for cars and trucks that are sold to the public.

[72] Rafter, *supra* note 68.

[73] *U.S. will not seek to require event data recorders in cars, trucks*, REUTERS (Feb. 5, 2019), https://www.reuters.com/article/us-usa-autos-regulations/u-s-will-not-seek-to-require-event-data-recorders-in-cars-trucks-idUSKCN1PU2GK.

[74] Rafter, *supra* note 68.

[75] *See* Joseph C. Baiocco, et. al, *Driver Privacy Act of 2015 Addresses Privacy Concerns for Data Collected on Event Data Recorders*, NATIONAL LAW REVIEW (Mar. 2, 2016), https://www.natlawreview.com/article/driver-privacy-act-2015-addresses-privacy-concerns-data-collected-event-data [hereinafter The National Law Review] (detailing the exceptions as to when the data collected by EDRs does not belong to the owner or lessee of

Manufacturers use the data for the EDR to improve vehicle safety features and, in the event where someone claims that the vehicle did not perform as designed during a crash, the manufacturer uses the EDR data to prove the vehicle was operating properly.[76] Since drivers own their vehicles, they own the data the vehicles generate including the EDR.[77] According to Tom Kowalick, chair of an EDR standards working group for the Institute of Electrical and Electronic Engineers who wrote information on EDRs for the NHTSA, "state troopers could get the data without a subpoena if there was a fatality. If they want to grab it, there's nobody saying they can't."[78]

2. Fourth Amendment Implications in the U.S.

Since the EDR continuously records as the vehicle travels, the data is only stored if a major event occurs such as a crash or an airbag deployment.[79] The data found in the EDR would be incredibly helpful to an investigator attempting to reconstruct the crash/incident and determine whether the driver was negligent or reckless while driving, or even whether the driver committed the crash intentionally (intending to kill the victim).

Obtaining the EDR records stored in the car would be similar to obtaining a driver's diary located inside the car describing the driver's intentions and observations before, during, and after the crash: "I didn't buckle my seatbelt . . . I accidentally pressed the accelerator instead of the brake . . . I was going really fast . . . I adjusted my seat while driving in order to look for my cell phone right before the crash . . . " Is this type of data similar to data found on a person's cell phone? Or is it less personal, less informative, less revealing?

The answer to that question is critical because it will determine whether the data found in the EDR falls under Fourth Amendment protection and whether investigators should be required to obtain a search warrant before accessing such data. In *Riley v. California*, a police officer arrested Riley and seized a cell phone from his pants pocket. The officer accessed the

---

the motor vehicle).

[76] *Id.* ("Since 2020, the National Highway Traffic Safety Administration has regulated (NHTSA) has regulated EDRs.") The Act establishes the owner or lessee of a motor vehicle as the owner of data collected and stored on the vehicle's EDR, however there are exceptions. These limited exceptions include (1) as authorized by a court or judicial or administrative authority, subject to the standards for admission into evidence; (2) pursuant to the written, electronic or recorded audio consent of the vehicle owner or lessee; (3) to carry out investigations or inspections authorized by federal law.

[77] Driver Privacy Act, 129 Stat. 1712 (2015) (codified as amended at 49 U.S.C. § 30101-30183 (2015)).

[78] Rafter, *supra* note 68.

[79] The National Law Review, *supra* note 75.

information on the phone without obtaining a warrant and used several photographs found in the phone to convict him at trial. The Supreme Court pointed out several reasons why police officers should obtain a warrant before searching a person's cell phone:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person . . . many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, Rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers . . . The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record . . . . The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. [Second], the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone . . . . A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form – unless the phone is.[80]

Is the EDR similar to a cell phone? Since the data in the EDR reveals only a few seconds of driving information, such data is arguably much more limited and less revealing than the data accessible from a cell phone. However, despite its limitations, the data in the EDR can reveal highly inculpatory evidence of negligence, recklessness, or intent on behalf of the driver. And since the EDR is located inside the vehicle (a driver's "effect"), it could be argued that the investigator would need to obtain a warrant to access the personal "effect" of the driver as it contains potential evidence of the defendant's guilt.

---

[80] Riley v. California, 573 U.S. 373, 394–97 (2014).

On the other hand, the automobile exception exists to allow for warrantless searches in cases when the officer has probable cause to believe the evidence of a crime or contraband could be found inside the car. Would the fact that a crash occurred be enough to argue probable cause exists to extract the EDR from the vehicles involved in the crash? Is there probable cause to believe a crime (e.g., negligent driving) occurred based on the fact the crash occurred? Perhaps if a fatality occurred, police should have the right to extract data from all EDRs involved in the accident.[81]

All traffic investigators are cognizant of EDRs and would likely want to seize an EDR before the data is erased. Perhaps the compromise in this scenario is to allow the investigator to seize the EDR at the time of the crash and seek a warrant to obtain and analyze the data inside. The data found in the EDR is detailed, accurate, and highly personal, and relevant to the driver's actions before, during, and after the crash. Using this data trial warrants immediate seizure and subsequent search warrant requirements to access and process to eliminate future chain of custody issues. However, the facts to justify probable cause should not be so high to limit investigators' ability to access EDR data in the event of a pedestrian or passenger fatality. If an investigator can demonstrate alcohol or drugs may have been a factor in the accident, or evidence if tire marks or accident reconstruction tools are used to demonstrate someone may have been negligent in their driving, there should be enough facts to support a probable cause standard to access the EDR's data.

Lastly, criminal investigators may argue the special needs exception to the warrant requirement applies and that they can have access to EDR data obtained by NTSB officials. According to the Driver Privacy Act of 2015, NTSB officials may seize and access an EDR while conducting research for traffic safety purposes and may stumble upon evidence in the EDR that points to a driver's negligence or recklessness while driving.[82] Can the NTSB official, while conducting a non-criminal investigation to improve highway safety and monitor vehicle functions, pass this data to a criminal investigator building a case against the driver? According to the Supreme Court in *New York v. Burger*, the government official who originally obtained the information without a warrant must advance a "substantial interest" and justify the warrantless intrusion as necessary to further the regulatory

---

[81] *See* Lindsey Barrett, *Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception*, 106 GEORGETOWN L.J. 181, 194–95 (2017) (discussing how the automobile exception might apply to data collected via connected cars and automated vehicles).

[82] S. REP. NO. 114-147 (2015), ("By clarifying that the owner or lessee of a vehicle is also the owner of any information collected by an EDR, [The Driver Privacy Act of 2015] would greatly enhance the personal privacy of these individuals.").

scheme.[83] The ordinance or statute that permits the warrantless inspection must provide an adequate substitute for the warrant that limits the discretion of the official regarding the time, place, and scope of the search.[84] By justifying the search using a non-criminal "regulatory" reason, government officials can access the data and essentially pass on relevant, incriminating data to criminal investigators.[85] This secondary reason (to gather evidence and file criminal charges against a defendant) was incidental to the purposes of the administrative search.[86]

In *Burger*, New York had statutory regulations that required automobile junkyards to obtain a license, display their registration number, maintain a record of the automobiles and parts in their possession, and allow police officers to inspect their records and inventory.[87] The state's substantial interest was "in regulating the vehicle-dismantling and automobile-junkyard industry because motor vehicle theft has increased in the State and because the problem of theft is associated with this industry."[88] Police officers conducted an inspection and found numerous stolen vehicles and parts in the junkyard owner's possession.[89] The police could use the evidence acquired during the inspection to also criminally prosecute the owner. Just because "the ultimate purpose of the regulatory statute pursuant to which the search is done" and the purpose behind a criminal prosecution "deterrence of criminal behavior" was the same, the officer could still use the evidence in a criminal trial.[90]

Similarly, criminal investigators who do not have enough to support a probable cause finding for a warrant may find some reprieve if NTSB officials obtained the EDR data for some other reason by other means. Moreover, other exceptions to the warrant requirement other than the automobile and special needs exceptions need to be explored. Could criminal investigators arrest someone for drunk driving and then pull the EDR data from the vehicle, arguing there was reason to believe evidence of the crime for which the defendant was arrested would be found on the EDR (search incident to lawful arrest exception)?[91] Could Customs agents at a border checkpoint retrieve EDR data from the vehicle as part of the border search exception?[92]

---

[83] New York v. Burger, 482 U.S. 691, 692 (1987).
[84] *Id*.
[85] *Id.* at 702.
[86] *Id*. at 727–28.
[87] *Id.* at 704.
[88] *Id*. at 708.
[89] *Id*. at 695–96.
[90] *Id*. at 693.
[91] *See* Arizona v. Gant, 556 U.S. 332, 335 (2009).
[92] *See* United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

C. Data Collected by the Autonomous Vehicle Company

1. Existing Technology

The third category of data being collected and processed is connected car data—data that flows wirelessly between a network of car manufacturers, vendors, and other third parties[93] to provide services for vehicle owners and to improve the car's artificial intelligence and effectiveness on the road.[94] The various technologies found in modern cars today "enable them to access information via the internet and gather, store, and transmit data for entertainment, performance, and safety purposes."[95] Vehicles can now be equipped with vehicle-to-vehicle (V2V) communications technology to communicate with other cars[96] and with traffic light cameras and ALPRs. Transponders are placed in cars to send their ID via radio to toll booths; emergency services such as OnStar are wirelessly connected to vehicles to provide roadside assistance and preventative maintenance reminders; satellites inform drivers of their location and offer navigation services; fleet operators can communicate with an AV through a third party monitoring

[93] Connected car data also includes data found in the infotainment system (to include when a driver accessed entertainment and navigation apps), data found in the phone-projecting software which mirrors the apps being used from your smartphone, and data from the smartphone itself which is connected to the car via Bluetooth, Wi-Fi or USB. "Infotainment" features include in-car apps, telephone and text connectivity, and in-vehicle internet connectivity. *See* Joseph Jerome, *Mobile and the Connected Car*, (Feb. 26, 2013), https://fpf.org/blog/mobile-and-the-connect-car/.

Auto insurance companies provide "dongles" that connect to a port and collect and transmit consumer data such as the owner's driving habits. Insurance companies can use this information to determine rates and insurance discounts for consumers that exhibit safe driving. *See* National Automobile Dealers Association and the Future of Privacy Forum, CONSUMER REPORT: PERSONAL DATA IN YOUR CAR 4, (Jan. 2017), https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf [hereinafter DATA IN YOUR CAR] ("Owners may also choose to plug in a third party-device (or "dongle") into the OBD-II port in some vehicles to collect or share information about their vehicle with third parties of their choice (for example, with their insurance company in order to gain safe driving discounts). Accessible information may include driver behavioral information (how fast you drive, how aggressively you apply the brakes, etc.) as well as geolocation data (where you are, where you have traveled, and your speed).").

[94] *Connected Cars*, FUTURE OF PRIV. F., https://fpf.org/issue/connected-cars/ (last accessed Mar. 10, 2022).

[95] FED. TRADE COMM'N, THE CONNECTED CARS WORKSHOP: THE FEDERAL TRADE COMMISSION STATE PERSPECTIVE 1, (Jan. 2018), https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf.

[96] *Id.*

device; and car makers receive all the data from the electronic control units, infotainment system, and the AV's constant imaging and scanning (to include LIDAR, radar, ultrasonic sensors, and cameras).[97]

The investigator can learn quite a bit from all the data collected inside the car and transmitted to third parties. The investigator can learn about the vehicle's operations and functions, including maintenance status and mileage; the driver's physical characteristics or how they drive, including their speed, seat belt use, and braking habits; the vehicle's precise location; and the personal accounts established by the vehicle owner.[98]

On a simple trip to the grocery store, the navigation system will collect the location of your vehicle at all times and your requested destination as it guides you to the store.[99] The car may already have physical or biometric information on you and adjust vehicle systems according to your personal preference.[100] Before even turning on the ignition, the vehicle may adjust the seat automatically after your face is recognized by a sensor located in the vehicle.[101] The car's cameras, sensors, and technologies such as blind-spot detection, lane departure warnings, assisted braking, and rear-parking detection, will be gathering information about your immediate surroundings as you travel to the store, including the current weather conditions, lane markings and obstacles, and nearby traffic.[102] Sensors, microphones, and cameras will record you inside the car as you communicate and interact with third-party systems like Apple CarPlay or Android Auto and use music apps on your phone, access your contacts, and make hands-free phone calls.[103] Your personal contact information has already been downloaded when you "synced" your phone with your vehicle.[104] The user recognition software is also tracking your eye movement to detect your attention level and whether you might fall asleep behind the wheel.[105] On your way back home from the store, your garage door has been programmed to be opened using the car's Bluetooth capabilities.[106] You are now home and ready to bring your bag of groceries into your "smart" home filled with "smart" appliances ready to accommodate your every need and meanwhile, collect even more data on

---

[97] *Infographic: Data and the Connected Car,* FUTURE OF PRIV. F. (Jun. 29, 2017), https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

[98] *Id.*

[99] DATA IN YOUR CAR, *supra* note 93, at 5.

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.* at 7.

[105] *Id.* at 5.

[106] *Id.* at 7.

your personal habits (preferred room temperature, lighting conditions, and Netflix shows, etc.).

According to the National Automobile Dealers Association, "[a]utomakers are already responsible and trusted stewards of vehicle data."[107] Those in the automotive industry that are part of the Alliance of Automobile Manufacturers developed Automotive Consumer Privacy Protection Principles in 2014 and have affirmed that manufacturers will: (1) be transparent and provide vehicle owners with "clear and concise privacy policies;" (2) require owner's consent before certain sensitive information (such as geolocation, biometric data, or driver behavior data) "is used for marketing or shared with unaffiliated third parties for their own use;" and (3) clearly state the circumstances when they will share owner's information with law enforcement.[108]

California has been a leader in giving consumers more control over the personal information that businesses collect about them. The California Consumer Privacy Act of 2018 (CCPA) requires businesses to give their customers certain notices explaining their privacy practices, to include (1) the right to know about the personal information a business collects about them and how it is used and shared, (2) the right to delete personal information collected from them,[109] and (3) the right to opt-out of the sale of their personal information.[110]

The NHTSA has "broad regulatory authority over the safety of" vehicles, and the Federal Trade Commission (FTC) is "responsible for protecting consumer privacy."[111] The NHTSA and FTC regularly coordinate and collaborate on "privacy issues related to motor vehicles" and technologies associated with connected and automated driving systems.[112] The FTC has the power "to bring an action against an automaker that uses a consumer's personal data in a way that violates the manufacturer's stated privacy policies."[113] In 2017, the U.S. Department of Transportation and the NHTSA released new federal guidance for automated vehicles, *Automated*

---

[107] *Id*. at 6.

[108] *Id*. *See also Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*, ALL. FOR AUTO. INNOVATION (Mar. 21, 2019), http://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

[109] There are some exceptions that allow businesses to keep a customer's personal information. For instance, the act does not apply to medical information protected by HIPAA, California Consumer Privacy Act, CAL. CIV. CODE § 1798.146(a)(1), or information collected, used, or disclosed in research under the Common Rule. CIV. § 1798.146(a)(5).

[110] CIV. § 1798.135(a)(1).

[111] DATA IN YOUR CAR, *supra* note 93.

[112] *Id.*

[113] *Id.*

Driving Systems 2.0: A Vision for Safety, and reiterated that "privacy considerations are critical to consumer acceptance of ADS and should be taken into account throughout the design, testing and deployment process."[114]

Congress has not enacted any federal legislation surrounding the privacy implications of the vast amount of data collected in automated vehicles. A bill entitled the SELF DRIVE Act was introduced in the House in September 2017 and again in 2020 "to clarify the Federal role in ensuring the safety of highly automated vehicles as it relates to design, construction, and performance, by encouraging the testing and deployment of such vehicles."[115] The bill requires auto manufacturers to develop a cybersecurity plan to detect and respond to cyber attacks and potential hacking into the ADS,[116] and demands that the Secretary of Transportation "determine the most effective method" for informing consumers about the capabilities and limitations of an automated vehicle and requires manufacturers to do so.[117] Lastly, the bill requires that auto manufacturers develop a "privacy plan with respect to the collection, use, sharing, and storage of information about vehicle owners or occupants collected by a highly automated vehicle" and their method for "providing notice to vehicle owners . . . about the privacy policy."[118] The bill also requires the Secretary of Transportation to create a Highly Automated Vehicle Advisory Council,[119] and the FTC to conduct a study as to which manufacturers have privacy plans and the "disclosures made . . . regarding the collection, use, sharing, and storage of vehicle owner or occupant data."[120]

---

[114] *Vehicle Data Privacy*, NAT'L. HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy#resources (last visited Mar. 13, 2022).

[115] Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act, H.R. 8350, 116th Cong. § 2 (2020). *See* also Alexandra Green, Case Note, *The Self Drive Act: An Opportunity to Re-Legislate a Minimum Cybersecurity Federal Framework for Autonomous Vehicles*, 60 SANTA CLARA L. REV. 217, 218–21 (2020) (discussing background of the SELF DRIVE Act). The bill, originally numbered H.R. 3388 and currently H.R. 8350, was introduced by Rep. Robert Latta (R-OH), chairman of the House Subcommittee on Digital Commerce and Consumer Protection.

[116] H.R. 8350, 116th Cong. §§ 4(b)(1), 5(a) (2020).

[117] *Id.* § 8.

[118] *Id.* § 12(a)(1–2).This privacy plan will include "the practices of the manufacturer with respect to the data minimization, de-identification, and retention of information about vehicle owners or occupants." *Id.* § 12(a)(1)(C). If the information about vehicle owners or occupants can not reasonably be linked to the AV or the information is anonymized or encrypted, the manufacturer is not required to include the practices regarding that information in the privacy policy. *Id.* § 12(a)(3–4).

[119] *Id.* § 9(a).

[120] *Id.* § 12(b)(2–3).

2. Fourth Amendment Implications in the U.S.

Criminal investigators, particularly those determining criminal liability in traffic accidents (drunk driving, hit-and-run, negligent driving, and intentional vehicular homicide), will hit a goldmine when they access the data auto manufacturers store, process, and analyze. Imagine receiving a USB containing the car's precise location at all times, its speed, photos and videos of what was going on inside and outside the car, audio recordings of verbal commands given to the car, how many passengers were in the car, how many seatbelts were fastened, and even how wide open the sunroof was[121]—not to mention the data from connected cell phones (what numbers were dialed, how long the conversations lasted, when a text message was sent or received, when a podcast app was activated, what was accessed on the phone, etc.). Vehicle systems forensics are used with increasing frequency by law enforcement to access and utilize the plethora of vehicle data that is gathered from highly or fully automated vehicles and stored by third parties.

What should be required to access the data transmitted to a company's data storage center? The first option could be that the data falls under the third-party doctrine, requiring nothing from the investigator other than simply asking the car company for the data (or handing the company a subpoena on behalf of a grand jury or an administrative subpoena and asking for the data). The third-party doctrine, as laid out in *Smith v. Maryland,* can be triggered when a person chooses to use the services/product of a third party, and the third party collects information to satisfy its obligations to the customer.[122] In the case of Smith, he chose to use telephone services, and therefore, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[123] When using a third party's services, one must assume the risk that the company will reveal to police the information the company has obtained, which in this case was the phone numbers Smith dialed.[124] The Supreme Court put a few limitations on the third-party doctrine in that the information requested must not reveal "the contents of communications."[125]

---

[121] Otonomo, BMW CARDATA 5 (2020), http://cdn2.hubspot.net/hubfs/7111373/PDF/OOOO_BMWData.pdf (last accessed Mar. 22, 2022). BMW CarData connects their vehicles in Europe to a system that automatically sends information about the status of the vehicle to selectable third parties every time the doors are opened or key is turned in the ignition/every three minutes depending on the model. The information includes the speed, the mileage of the vehicle, the number of seatbelts buckled, the longitude and latitude coordinates of the vehicle, the status of open windows, etc.

[122] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[123] *Id.* at 744.

[124] *Id*. at 744–45.

[125] *Id*. at 741.

Smith would have a reasonable expectation of privacy in the content of his conversations but not metadata such as the telephone numbers he dialed so that the phone company's switching equipment can get the recipient on the phone. Also, the company must have a reason for keeping these records, just as the phone company in *Smith* kept a record of the numbers he dialed to check billing operations (customers were eligible for special rate structures based on the number of calls they made), detect fraud, and prevent violations of law.[126]

Law enforcement has embraced the use of the third-party doctrine to access company records through the use of a simple subpoena requesting such information. Subpoenas can be used to access bank records, credit card records, frequent flier program records, customer loyalty accounts, email or phone subscriber information, hospital admission records, toll records, and whatever else might be described as a "transactional record."[127] So much data is being collected every time we access the internet, buy items, enter chatrooms, and utilize apps on our phones, that it led Justice Sotomayor to reconsider the third-party doctrine in *Jones*.[128]

The Supreme Court provided further clarification and placed additional limitations on the third-party doctrine in its decision in *Carpenter v. United States* in 2018.[129] Investigators had requested cell-site location information (CSLI) obtained from a company's cell phone records via a court order, which requires that the records sought "are relevant and material to an ongoing investigation" and not from a warrant, which would require facts to support a probable cause showing that a crime is ongoing or has been committed.[130] To support the argument that CSLI should fall under the third-party doctrine, the government could argue based on the *Smith* decision (1) that cell phone carriers have a business purpose to keep CSLI, "including finding weak spots in their network and applying 'roaming' charges when another carrier routes data through their cell sites," and (2) that CSLI is like metadata and does not reveal the content of any communication that happens on the cell itself.[131]

---

[126] *Id*. at 742.

[127] Am. Bar Ass'n, ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD-PARTY RECORDS (3d ed. 2013).

[128] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[129] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[130] *Id.* at 2212 (Prosecutors had applied for a court order under the Stored Communications Act to obtain cell phone records which would indicate Carpenter's cell-site location during a four-month period. The government was required to offer specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation.).

[131] *Id.* at 2212, 2218–19. In fact, the Sixth Circuit found that Carpenter lacked a reasonable expectation of privacy in the location information because he had voluntarily

The real issue in *Carpenter* lies in how one feels about the collection of four months' worth of CSLI—is the cell-site location information like a telephone number dialed or a bank record, or does a person maintain a reasonable expectation of privacy in their cell's (and presumably their own) location similar to how they would feel about a private cell phone conversation they might have?

The Court decided that CSLI is "detailed, encyclopedic, and effortlessly compiled."[132] It is not like a bank record "but a detailed and comprehensive record of the person's movements."[133] "[A] cell phone—almost a 'feature of human anatomy'—tracks nearly exactly the movements of its owner."[134] Moreover, to live and communicate with others in today's society, one must accept the fact that it is necessary to use a cell phone. "[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[135] And CSLI will be collected whether the user likes it or not. "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[136]

Therefore, the Court determined that cell phone location records can be "deeply revealing," and "its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection" make it inaccessible to law enforcement to obtain under the third party doctrine.[137] Investigators would need a warrant to access such data from a cell phone provider.

Carpenter is incredibly important to understand as we analyze the data investigators wish to obtain from third parties associated with AV businesses. The government could argue that (1) auto manufacturers have a business purpose for storing and analyzing all the data being collected—they

---

shared that information with his wireless carrier as "a means of establishing communication." *Id.* at 2213.

[132] *Id*. at 2216. "Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the 'privacies of life.' And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense." *Id.* at 2217.

[133] *Id*. at 2217.

[134] *Id*. at 2218.

[135] *Id*. at 2210 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[136] *Id*. at 2220 ("As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (quoting Smith v. Md., 442 U.S. 735, 745 (1979))).

[137] *Id*. at 2223.

are consistently making improvements in autonomous cars and determining whether the vehicle is functioning properly, and manufacturers want to ensure compliance with safety standards as more and more vehicles become partially and fully automated. But, factor (2), that the data collected is like metadata and that a person does not have a reasonable expectation of privacy in the data being collected, is a relatively weak argument, especially considering that a vehicle's location information is very similar to CSLI collected by a cell phone company. However, the government can argue that the Court in *Carpenter* distinguished CSLI from tracking devices placed on automobiles that reveal a vehicle's location. "While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[138] Perhaps the government might persuade the Court that information on a vehicle is not as revealing as what is found on a person's cell phone.

On the other hand, defense attorneys can argue that car data is like CSLI in that it gives "police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention [policies] of the wireless carriers, which currently maintain records for up to five years."[139] Current data collected by car companies is like data collected by cell phone providers: "they are ever alert, and their memory is nearly infallible. There is a world of difference between . . . limited types of personal information . . . and the exhaustive chronicle of location information casually collected by wireless carriers today."[140]

There is also a question as to whether drivers and passengers in the car are voluntarily conveying the data collected by car companies. The *Carpenter* Court was skeptical that cell phone users knowingly or voluntarily were sharing their cell-site location information with their cell providers.[141] A cell phone automatically keeps track of its location without the user having to do anything.[142] Is the driver aware of all the data being collected every time he or she turns on the engine? Do we need to give up our cars and take public transportation to avoid our driving and travel data from being collected? We must determine what exactly the driver is voluntarily conveying and whether

---

[138] *Id*. at 2218.
[139] *Id*.
[140] *Id*. at 2219.
[141] *Id.* at 2210.
[142] *Id.* at 2220.

cars are "indispensable to participation in modern society"[143] to determine whether the third party doctrine even applies to such data.

The bottom line is that digital information is different from the data of yesterday. There is no denying the amount of data collected by car companies is "detailed, encyclopedic, and effortlessly compiled." As described above, the data collected is highly sensitive, and the driver and others in the car do not voluntarily expose their activities inside the car for all to view (compared to external activities captured by surveillance cameras outside the car). [144] If a criminal investigator wants access to these detailed records, audio, video, vehicle operations, driver functions, and location information, they must get a warrant. Just as *Riley* almost certainly required a warrant to search a cell phone.[145] If law enforcement wants to monitor a vehicle (and those inside the vehicle) and watch and listen to those inside the vehicle in real-time, they should apply for a Title III wiretap[146] just as they would if they wanted to listen in on a person's phone conversations in real-time. If a criminal investigator wants location information in real time or historical information on where a vehicle has been in the past, whether that be in the days or weeks, or months leading up to a crash, auto incident, or ongoing crime, the agent needs a warrant. At the very least, this will serve as a judicial check on the agent's power and will require law enforcement to articulate a strong need and reason for accessing such pervasive and sensitive personal information.[147]

III. SURVEILLANCE CAR DATA'S IMPACT IN A LEVEL 3 WORLD VERSUS A LEVEL 5 WORLD

On March 18, 2018, at 10 p.m., the Tempe Police and Fire Departments were called to the scene of a car accident and pedestrian fatality in Tempe, Arizona.[148] Upon arrival, police learned that Rafaela Vasquez, an

---

[143] *Id*. (citing *Riley*, 573 U.S. at 385).

[144] Interestingly, the Supreme Court in *Carpenter* made clear that its decision as to whether CSLI falls under the third-party doctrine should have no impact on previous decisions on "conventional surveillance techniques and tools, such as security cameras." *Id*. at 2210.

[145] Riley v. California, 573 U.S. 373, 385 (2014).

[146] 18 U.S.C. § 2511 (2021).

[147] I would, however, allow for an emergency exception under the exigent circumstances exception to the warrant requirement. *Brigham City, Utah v. Stuart,* 547 U.S. 398 (2006). If a crime is in progress, i.e., someone has been kidnapped, someone is on their way to commit a murder or armed robbery, etc., law enforcement should be able to access the car's data in real time to prevent to violent crime from occurring. Law enforcement can follow up by later applying for a search warrant to justify the immediate access to the data.

[148] NATIONAL TRANSPORTATION SAFETY BOARD, COLLISION BETWEEN VEHICLE CONTROLLED BY DEVELOPMENTAL

automated vehicle operator for Uber since June 2017, had been in the driver's seat of a Volvo XC90 SUV equipped with an ADS.[149] The pedestrian, Elaine Herzberg, had attempted to cross a darkened stretch of road while pushing her bicycle.[150] The vehicle, on a test run, noticed Herzberg via radar for 5.6 seconds before impact, but because she was not riding her bike but merely walking beside it, the vehicle's radar system only registered her first as an unknown object, then a car, then a bicycle with varying predictions as to where the object/car/bicycle may go next.[151]

The National Transportation Safety Board (NTSB) investigators later learned that Uber's technology in the car did not have "the capability to classify an object as a pedestrian unless that object was near a crosswalk," and Herzberg had not been in the crosswalk.[152] Records from the streaming service Hulu also revealed that Vasquez, the "back-up" driver, was watching the reality show, *The Voice*, on her cellphone for 12.5 seconds before the crash and did not hit the brakes until after the car struck Herzberg.[153] Investigators used the car's data to determine that the car was traveling at least 40 miles per hour along the eight-lane road.[154] They concluded the probable cause of the crash was "the failure of the vehicle operator to monitor the driving environment and the operation of the automated driving system

---

AUTOMATED DRIVING SYSTEM AND PEDESTRIAN, TEMPE, ARIZONA, MARCH 18, 2018, Highway Accident Report, NTSB/HAR-19/03, at 1 (2019), https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1903.pdf [hereinafter NTSB-HAR 19/03].

[149] *Id.* at 8 ("[The ADS] installed on the SUV was designed to operate in autonomous mode only on premapped, designated routes. When the ADS was active, it performed all driving tasks, including changing lanes, overtaking slow-moving or stopped vehicles, turning, and stopping at traffic lights and stop signs. Although the system was designed to be fully automated along a specific route, a human operator inside the vehicle was tasked with overseeing the system's operation, monitoring the driving environment, and if necessary, taking control of the vehicle and intervening in an emergency.").

[150] *Id.* at 1.

[151] *Id. See* Kea Wilson, *Driver of 'Driverless' Car Charged in 2018 Ped Death*, STREETSBLOGUSA (Sept. 16, 2020), https://usa.streetsblog.org/2020/09/16/human-driver-of-driverless-car-charged-in-2018-ped-death/#:~:text=E%2Dtaxi%20driver%20Rafaela%20Vasquez,killed%20pedestrian%20Elaine%20Herzberg%2C%2049 (citing to NTSB-HAR 19/03); *see also* Phil McCausland *Self-driving Uber Car that Hit and Killed Woman Did Not Recognize that Pedestrians Jaywalk*, NBCNEWS (Nov. 9, 2019), https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281.

[152] The NTSB report also later showed that Uber that disabled the automatic emergency braking functions of the vehicle to prevent sudden stops and potential rear-end crashes, and the forward collision warning technology had been deactivated which would have alerted the driver of a possible human being in the road. The NTSB investigates causes of accidents, whether it involves cars, boats, or airplanes.

[153] Wilson, *supra* note 151.

[154] NTSB-HAR 19/03, *supra* note 148, Figure 1 at 2.

because she was visually distracted throughout the trip by her personal cell phone."[155] Moreover, Uber "did not adequately recognize the risk of automation complacency and develop countermeasures to control the risk of vehicle operator disengagement, which contributed to the crash."[156]

On August 27, 2020, a Maricopa County grand jury charged Vasquez with negligent homicide.[157] The indictment stated it was a dangerous felony because the offense involved the use of a motor vehicle, a deadly weapon, or dangerous instrument and/or the intentional or knowing infliction of serious injury upon Herzberg.[158] The prosecutor involved in the case stated, "distracted driving is an issue of great importance in our community. When a driver gets behind the wheel of a car, they have a responsibility to control and operate that vehicle safely and in a law-abiding manner."[159] Vasquez is the first driver in human history to be liable for a pedestrian death involving an autonomous car.[160]

In an accident involving an Automated Driving System (ADS) such as Uber's Volvo SUV, what are some tools investigators have at their disposal to piece together what happened that night? Uber's SUV was equipped with numerous systems and modules able to record data. According to the NTSB's report,

---

[155] *Id.* at 43–44 ("[H]ad the vehicle operator been attentive, she would likely have had sufficient time to detect and react to the crossing pedestrian to avoid the crash or mitigate the impact . . . [t]he vehicle operator's prolonged visual distraction, a typical effect of automation complacency, led to her failure to detect the pedestrian in time to avoid the collision.").

[156] *Id*. at 44.

[157] Indictment, State v. Vasquez, No. CR2020-001853-001 (Super. Ct. AZ, Maricopa County).

[158] *Id.*

[159] MARICOPA COUNTY ATTORNEY'S OFFICE, *Grand Jury Indictment Returned on Rafael (aka Rafaela) Vasquez,* MARICOPA COUNTY ATTORNEY'S OFFICE CIVIC ALERT, (Sept. 15, 2020), https://www.maricopacountyattorney.org/CivicAlerts.aspx?AID=751.

[160] NTSB-HAR 19/03, *supra* note 148, at 19–20 (ATG records show that "between September 2016 and March 2018 (excluding the Tempe crash), 37 crashes and incidents involved ATG test vehicles operating in autonomous mode. Most (33) involved another vehicle striking the test vehicle. . . . In two incidents, the ATG test vehicle was the striking vehicle. In one, the ATG test vehicle struck a bent bollard in the bicycle lane that partly encroached on the vehicle's travel lane. In the other, the operator took control to avoid an oncoming vehicle that had entered the test vehicle's lane of travel; the operator steered away and struck a parked car. In the remaining two incidents, the ATG test vehicle was vandalized by a passing pedestrian while the vehicle was stopped."). Vasquez's defense team has argued that Uber should be held criminally liable instead of Vasquez for failing to put appropriate safety measures in place. Ray Stern, *Was the Backup Driver in an Uber Autonomous Car Crash Wrongfully Charged?*, PHOENIX NEW TIMES (July 9, 2021), https://www.phoenixnewtimes.com/news/uber-self-driving-crash-arizona-vasquez-wrongfully-charged-motion-11583771.

> The ADS that controlled the SUV at the time of the crash consisted of multiple systems for monitoring and analyzing the vehicle's performance and the surrounding environment. Each system had hardware components and software analysis and data-recording elements . . . [S]tructural components included (1) a lidar (light detection and ranging) system, (2) a radar system, (3) a camera system, and (4) telemetry, positioning, monitoring, and telecommunication systems.[161]

These autonomous cars are not equipped with just one camera but a dash-camera system that includes a forward-facing camera and an inward-facing camera for monitoring the vehicle operator.[162] Uber also installed a human-machine interface (HMI), much like a tablet computer, that enables interaction between the human in the vehicle and the ADS.[163] Essentially, the car is recording and monitoring the environment outside, around, and inside the SUV. As the vehicle travels, the sensors continually scan the environment and monitor vehicle dynamics, thereby verifying the vehicle's position.[164] Uber's Advanced Technologies Group provided NTSB investigators with extremely detailed information, including what was programmed before the trip, the data pertaining to the operator's interaction with the HMI, videos recorded by the cameras, sensor, and vehicle dynamics information, and quantitative data recorded by the ADS during the approximately 39-minute operation of the vehicle.[165] This data allowed investigators to identify the time the system detected the pedestrian, how the ADS predicted paths to the pedestrian and the actions the ADS took.[166] This information was duplicated by what investigators could pull from the SUV's own event data recorder/storage system which records data immediately before and after the impact.[167]

Moreover, the videos from the cameras showed that about 15 minutes before the drive, Vasquez removed a cell phone from a backpack and placed it in the bottom of the center console below the HMI tablet and out of the

---

[161] NTSB-HAR 19/03, *supra* note 148, at 8.

[162] *Id.* at 11.

[163] *Id.*

[164] *Id.* (The environmental features and roadway characteristics detected by the system, along with the monitored vehicle dynamics, are matched to the features and characteristics along the pre-mapped route at those specific locations.).

[165] *Id.* at 14.

[166] *Id.*

[167] *Id.* at 20–21 ("Depending on the module, the recorded data spanned 8 to 15 seconds. . . . Investigators also examined data from the Volvo supplemental restraint system (SRS), which controlled and stored information about air bag deployment and nondeployment events triggered by sudden velocity changes.")

camera's view.[168] Vasquez appeared to be gazing toward the cell phone even before entering the public road. In fact, NTSB investigators managed to analyze Vasquez's glances during the entire 39-minute drive, and they found that she spent approximately 34 percent of her time gazing down toward the bottom of the center console.[169] During nearly three minutes before the crash, Vasquez looked toward the bottom of the center console 23 different times.[170] She returned her gaze to the road about one second before impact.[171] According to the ADS data, Vasquez initiated a steering maneuver only 0.02 seconds before hitting Herzberg.[172]

According to Uber's records, Vasquez had completed a 3-week training program and had consistently taken refresher classes which included driving skills and ADS operation.[173] She was familiar with the section of N. Mill Avenue where the crash occurred and had traveled on it while operating test vehicles in autonomous mode.[174] She had completed the designated route 73 times in autonomous mode since completing her training.[175]

Vasquez told NTSB investigators that she had placed a personal phone in her purse before driving and that her company phone was on the passenger seat at the time of the crash.[176] She also said that moments before the crash, she was attending to and interacting with the HMI.[177] NTSB investigators obtained Vasquez's cell phone records which showed that her cell phone was continually streaming a television show between 9:16 p.m. and 9:59 p.m. on March 18.[178] That period covered the entire 39-minute trip and the crash.

The investigators collected evidence from the SUV itself, from the information Uber collected in real-time, from the streaming service, and the cell phone provider. This evidence is enough for the prosecution to make the argument at trial that Vasquez was criminally negligent at the time of the crash. She should have been aware that looking at her cell phone rather than the road and not monitoring the driving system's operations would be a

---

[168] *Id.* at 18.

[169] *Id.* ("The maximum continuous duration of the operator's downward gaze was 26.5 seconds. That occurred on the same section of N. Mill Avenue where the crash occurred but about 23.5 minutes earlier, while the operator was completing the first loop of the route.").

[170] *Id.* ("Seven glances lasted at least 3 seconds, with the longest lasting 6.9 seconds. The operator began glancing down toward the bottom of the center console 6 seconds before impact, where she retained her gaze for the next 5 seconds.")

[171] *Id.*

[172] *Id.*

[173] *Id.* at 23.

[174] *Id.*

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] *Id.*

substantial and unjustifiable risk to human life.

A. Evidence collected from an AV and presented to a jury will paint a more accurate picture of what occurred at the time of the crash.

Presumably, during the criminal investigation of Rafaela Vasquez, police officers obtained a warrant to access all the data Uber's Advanced Technologies Group collected from the Volvo XC90 SUV and to access the vehicle's EDR (unless they obtained the information from NTSB investigators). Warrants were more than likely issued to obtain detailed cell phone information to show she accessed Hulu and was watching *the Voice* while in the driver's seat.

How would a jury feel about such data? Is the data more accurate than an eyewitness? Studies and research have shown that eyewitness testimony is incredibly persuasive when put before a jury yet also incredibly unreliable.[179] Our memories fade quickly over time, our minds tend to fill in the gaps and are amenable to an officer's subtle (or not so subtle) suggestions, and once we commit to what we think we saw at the time, we tend to stick to the story (correctly or incorrectly).[180] It may seem obvious that introducing digital evidence displaying the speed of the vehicle, how the AV processed the data at the time of the crash, and what the driver was doing (via cameras and sensors in the car) would seem accurate and reliable in the jury's eyes. And perhaps it is more reliable than an eyewitness' memory. Digital data does not fade over time; it is collected, stored, and retained for however long the car manufacturer wants to keep it.

However, prosecutors must be careful as to chain-of-custody issues that might arise since the data is either stored by the auto manufacturer or another third-party provider. Preservation letters should be immediately issued after the crash, and warrants requesting access to the data should come soon after. Digital data can be altered, modified, and/or deleted. Prosecutors must ensure they can account for the data's whereabouts and who had access to the data at all times to avoid suggestions at trial that the data was altered.

Moreover, the digital data tells the story from the perspective of that particular camera, particular sensor, particular vehicle function – just like body cameras on police officers, it does not tell the whole story.[181] Digital data and other sources can slowly piece together what happened at the time of the crash, but only circumstantially. Prosecutors must be careful not to jump to conclusions because of one camera's video footage or one vehicle

[179] Elizabeth F. Loftus, *The Incredible Eyewitness*, PSYCHOL. TODAY, Dec. 1974, at 117–18.

[180] *Id*.

[181] Seth Stoughton, *Police Worn Body Cameras*, 96 N.C.L. REV. 1363, 1408 (2008).

function's perspective.

That said, digital data from an AV is far superior to any other accident reconstruction tool out there. The days of relying on tire swerve marks and dirt tracks and interviewing witnesses to prove what happened will be over in a Level 3 or 5 world. However, investigators seem hesitant to rely on AV data alone. In the case of Tiger Woods' crash, officers said they would not base a citation just off the EDR's data.[182] When comparing an eyewitness' memory to an AV's data, the opposite should be true.

B. Humans may still be held criminally liable in Level 3 conditional automation and even in a Level 5 fully automated driving world.

Vasquez was in a fully autonomous vehicle yet was still criminally charged with negligent homicide. Will human beings remain liable for traffic accidents as humans slowly turn over driving controls to AVs and their artificial intelligence? Certainly, in a Level 3 conditional automation world (where a driver is a necessity but is not required to monitor the environment)[183], the driver will still be held criminally liable because the driver must be ready to take control of the vehicle at all times with notice. In Vasquez's case, the vehicle was fully automated (Level 5), but it was essentially "in training" and needed the driver to have the option to control the vehicle if the AV fails to detect and identify objects on the road (which it did).

Requiring some sort of driver monitoring and control means that criminal investigators will still need data to determine if the driver is criminally liable and what mental state applies to his or her actions at the time of the crash. Was the driver not paying attention and therefore, negligent when the car hit the pedestrian? In other accident scenarios, the investigator must determine whether the driver intended to run past the stop sign or was reckless when speeding in a thunderstorm and sending a text message.

In a Level 5 world where there is no driver and all humans become simply passengers in the vehicle, an accident would, quite frankly, be the AV's fault (or the manufacturer who created a faulty design). Common traffic violations like speeding or running a red light or stop sign would become things of the past since AVs would be programmed to follow traffic laws. The data auto manufacturers are currently collecting would not be as great an interest to law enforcement because such data would only be used in the event

---

[182] Andrew Beaton, *Tiger Woods's Car Accident Caused by Unsafe Speeding*, WALL STREET J. (Apr. 7, 2021),
https://www.wsj.com/articles/tiger-woods-update-crash-cause-investigation-speeding-injuries-11617816842.

[183] SAE, *supra* note 3.

the government wished to criminally prosecute the AV manufacturers for creating a "negligent" vehicle (such as failing to recognize pedestrians not following the crosswalk signs). AVs would not be programmed to cause accidents or harm other humans, but as artificial intelligence learns from its mistakes (as does a 16-year-old who just obtained his driver's license), so too will AVs make mistakes and cause traffic accidents. Regardless, law enforcement will always have an interest in the data obtained from car companies. (And car manufacturers may be incentivized not to keep data on drivers and their driving because of such law enforcement interest). Such data will help offer proof that a certain person was at a particular location at a particular time, that calls were made in the AV, or that a crime was captured on one of the AV's many audio and video recording devices. A search warrant should be necessary—even in a Level 5 world.

C. Expect more traffic accidents and criminal prosecutions in a Level 3 conditionally automated world as human drivers become complacent as AV systems take over most of the driving.

One of the greatest concerns we face moving from Level 3 to Level 5 automation is the impact on a human driver's capacity to pay attention and not be drawn into becoming too complacent/negligent in their driving responsibilities. The Pew Research Center surveyed in 2014 and found that 48% of all Americans surveyed were interested in riding in a driverless car.[184] The Ericsson ConsumerLab Analytical Platform conducted a survey on consumers' attitudes towards car driving and found that 47% percent of consumers indicated that they were interested in self-driving cars.[185] The common characteristics of those individuals who are the most interested in autonomous cars are white-collar professionals with children in the household and who already use a car to commute.[186] Almost half of all

[184] Aaron Smith, *U.S. Views of Technology and the Future*: *Science in the Next 50 Years*, PEW RESEARCH CENTER (Apr. 17, 2014), https://www.pewresearch.org/internet/2014/04/17/us-views-of-technology-and-the-future/. 59% of college graduates are interested in riding in driverless cars. *Id.*

[185] *The Self Driving Future: Consumer Views on letting go of the wheel and what's next for autonomous cars*, ERICSSON (Feb. 2017), https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/self-driving-future. "Further, one in four smartphone users states that they would prefer an autonomous car to one they drive themselves, despite the fact that autonomous vehicles are not yet part of everyday traffic. Additionally, 7 in 10 state an interest in self-driving car features, such as cruise control and parking assistance." *Id.* However, in an AutoPacific US study, "46% of respondents stated that they would not trust a computer to make driving decisions for them." *Id.* Therefore, "[c]onsumers' trust in the technology will have to gradually increase before they are ready for a fully autonomous future." *Id.*

[186] *Id.*

Americans can't seem to wait to hand over the controls to the car and spend their travel time doing other, more interesting (or more productive) things.

In fact, we have seen this phenomenon already played out in several recent accidents involving AVs. On a bright, sunny day on May 7, 2016, in Williston, Florida, Joshua Brown was killed in a Tesla Model S with Autopilot capabilities[187] when the car hit a tractor-trailer at a highway intersection.[188] The National Highway Traffic Safety Administration ("NHTSA") investigated the crash and found that the car's sensor system failed to distinguish a large white 18-wheel truck and trailer crossing the highway.[189] The car attempted to drive full speed under the truck, and the car hit the bottom of the trailer and the top of the vehicle was torn off from the impact.[190] Tesla's CEO Elon Musk said that the vehicle's radar "tunes out what looks like an overhead road sign to avoid false braking events."[191] Tesla has previously warned its customers that Autopilot is not an autonomous driving system and still requires constant attention to the road while in use.[192] The tractor-trailer driver said that Brown was watching a Harry Potter movie at the time of the crash, and the Florida highway patrol later found a portable DVD player in the vehicle.[193]

The NHTSA analyzed data supplied by Tesla for all 2014 through 2016 Model S and 2016 Model C vehicles equipped with Autopilot.[194] The data showed that the Tesla vehicle crash rate decreased by 40 percent after

---

[187] Peter Valdes-Dapena, *Tesla's New Autopilot is Amazing, But Please Keep Your Eyes on the Road*, CNN BUSINESS (Apr. 24, 2019), https://www.cnn.com/2019/04/22/success/tesla-navigate-on-autopilot/index.html. ("Autopilot software can take over most of the driving and "allows a car to change lanes on its own and even drive through highway interchange ramps itself while the driver's hands just hold the steering wheel.").

[188] Joan Lowy & Tom Krisher*, Tesla Driver Killed in Crash While Using Car's 'Autopilot'*, AP NEWS (Jun. 30, 2016), https://apnews.com/article/ee71bd075fb948308727b4bbff7b3ad8 ("The incident happened due to the failure of the autopilot software to detect the other vehicle and automatically activate the brakes").

[189] *Id*.

[190] Sam Levin & Nicky Woolf, *Tesla Driver Killed While Using Autopilot was Watching Harry Potter, Witness Says,* THE GUARDIAN (July 1, 2016), https://www.theguardian.com/technology/2016/jul/01/tesla-driver-killed-autopilot-self-driving-car-harry-potter.

[191] Andrew Hawkins, *Fatal Tesla Autopilot Accident Investigation Ends With No Recall Ordered*, THE VERGE (Jan. 19, 2017), https://www.theverge.com/2017/1/19/14323990/tesla-autopilot-fatal-accident-nhtsa-investigation-ends.

[192] Kim Lyons, *Two People Killed in Fiery Tesla Crash With No One Driving*, THE VERGE (Apr. 18, 2021), https://www.theverge.com/2021/4/18/22390612/two-people-killed-fiery-tesla-crash-no-driver.

[193] Levin & Woolf, *supra* note 190.

[194] *Id.*

Autopilot was installed.[195] It appears that when an AV is in control of driving (with humans supervising), the error rate is a lot lower than when humans are in control of driving. Autopilot had been installed on Brown's vehicle, and despite the AV's mistake (thinking that the tractor-trailer was a road sign instead of what it actually was), Brown would have still had seven seconds to see the truck and take some sort of action.[196] The NHTSA decided to exonerate Tesla and the Autopilot system and not issue any vehicle recalls.[197] Rather, the NHTSA took the opportunity to warn human drivers – "While ADAS [advanced driver assist systems] technologies are continually improving in performance in larger percentages of crash types, a driver should never wait for automatic braking to occur when a collision threat is perceived."[198] In other words, Autopilot may help in reducing auto accidents, but the human in the driver's seat will be ultimately responsible and, therefore, the human should continue to pay attention to the road.

Yet, humans are craving the opposite – they want to tune out the road and accede the driving responsibility to the Autopilot system. On April 17, 2021, in Spring, Texas, a Tesla 2019 Model S did not adhere to a curb and crashed into a tree and burst into flames, killing the two passengers inside the vehicle.[199] Local police said no one appeared to be behind the wheel, and one person was found in the passenger seat and the other in the back seat.[200] While Tesla has put safety measures in place to ensure a human driver is behind the wheel when Autopilot is activated,[201] Consumer Reports engineers tested Tesla's Model Y on a closed track and tricked it into operating in Autopilot without a driver present.[202] Tesla's CEO Elon Musk later tweeted that the Autopilot system was not enabled in the Texas crash and that the vehicle did

---

[195] Fred Lamber, *Tesla's Crash Rate was Reduced by 40% After Introduction of Autopilot based on Data Reviewed by NHTSA*, ELEKTREK.CO (Jan. 19, 2017), https://electrek.co/2017/01/19/tesla-crash-rate-autopilot-nhtsa/.

[196] Hawkins*, supra* note 191.

[197] *Id*.

[198] Hawkins, *supra* note 191 (citing NHTSA crash report, May 2016). In August 2021, the NHTSA launched an investigation into Tesla's self-driving Autopilot system after eleven Teslas using the feature crashed into emergency units responding to an incident on the highway. BBC (Aug. 16, 2021), https://www.bbc.com/news/technology-58232137.

[199] Lora Kolodny, *'No One was Driving' in Tesla Crash That Killed Two Men in Spring, Texas, Report Says,* CNBC (Apr. 19, 2021), https://www.cnbc.com/2021/04/18/no-one-was-driving-in-tesla-crash-that-killed-two-men-in-spring-texas-report.html.

[200] *Id.*

[201] TESLA SUPPORT, https://www.tesla.com/support/autopilot, (last visited June 27, 2021) (The driver's hands must be on the steering wheel every ten seconds or Autopilot disengages. The Autopilot feature also requires the driver's seatbelt to be buckled in order to be engaged).

[202] Cody Godwin, *Tesla's Autopilot Tricked to Operate Without Driver*, BBC NEWS (Apr. 23, 2021), https://www.bbc.com/news/technology-56854417.

not have Full Self-Driving [FSD] capabilities which would have allowed the use of Autopilot on local roads.[203]

The NHTSA is currently investigating 28 crashes involving Tesla vehicles.[204] NTSB Chairman Robert Sumwalt stated in a 2020 report, "There is not a vehicle currently available to U.S. consumers that is self-driving. Period. Every vehicle sold to U.S. consumers still requires the driver to be actively engaged in the driving task, even when advanced driver assistance systems are activated."[205]

Human drivers may become much more negligent as they accede many of their driving duties to the car. It is difficult to pay constant attention when we are actively driving much more so when we are not actively engaged in driving activities. There is no doubt that AVs will significantly decrease the number of traffic accidents and deaths on the road. In 2020, despite a pandemic leading many Americans to drive less, approximately 38,680 people died in the United States due to auto accidents, the highest since 2007.[206] An estimated 94 percent of auto accidents are caused by human error.[207] As some researchers have suggested, "humans must work in the sweet spot where manageable tasks keep them interested . . ." and that "[y]ou want to have enough workload that you maintain an adequate load of performance."[208] As Bryan Reimer, research at the MIT AgeLab and associate director of the New England University Transportation Center said, "It's not whether you want to attend or you don't want to attend. It's fundamentally in the back of the brain that you need a certain amount of demand to sustain attention."[209] If this is the case, that humans if given so few driving tasks are not simply capable of paying attention, should we criminally prosecute humans driving Level 3 to Level 5 AVs for negligent driving? Would a reasonable person in a Level 3 AV have been able to pay

---

[203] Elon Musk (@elonmusk), TWITTER (Apr. 19, 2021, 5:14 PM), https://twitter.com/elonmusk/status/1384254194975010826?s=20.

[204] Kolodny, *supra* note 200.

[205] Chris Isidore, *Police Say No One Was in Driver's Seat in Fatal Tesla Crash*, CNN BUSINESS (Apr. 19, 2021), https://www.cnn.com/2021/04/19/business/tesla-fatal-crash-no-one-in-drivers-seat/index.html.

[206] Press Release, National Highway Traffic Safety Administration, 2020 Fatality Data Show Increased Traffic Fatalities During Pandemic, (June 3, 2021), https://www.nhtsa.gov/press-releases/2020-fatality-data-show-increased-traffic-fatalities-during-pandemic.

[207] Press Release, National Highway Traffic Safety Administration, 2016 Fatal Motor Vehicle Crashes: Overview (October 2017) (available at https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812456).

[208] Keith Barry, *Too Much Safety Could Make Drivers Less Safe*, WIRED (July 27, 2011), https://www.wired.com/2011/07/active-safety-systems-could-create-passive-drivers/.

[209] Julia Guardione, *Is Too Much Technology a Bad Thing?*, RATEGENIUS (July 27, 2011), https://www.rategenius.com/is-too-much-technology-a-bad-thing/.

attention?

As Elon Musk stated on a May 2018 call with investors:

> When there is a serious accident it is almost always, in fact maybe always, the case that it is an experienced user, and the issue is more one of complacency. They just get too used to it. That tends to be more of an issue. It's not a lack of understanding of what Autopilot can do. It's [drivers] thinking they know more about Autopilot than they do.[210]

Vasquez was hired by Uber to supervise the AV's driving. Brown took numerous rides in his Tesla Model S and filmed many of his experiences using the Autopilot feature for future viewing on YouTube. The owner of the Tesla Model S in Texas, Dr. William Varner, decided to take a quick spin with his best friend and hopped in the back seat only to crash a few hundred yards down the road.[211] Perhaps car manufacturers and companies testing AV capabilities such as Uber should block streaming and internet services of their drivers.

Will the "reasonable person" over-trust this sort of technology like Vasquez, Brown, and Varner? Will juries who are unfamiliar with systems such as the Autopilot feature in the Tesla be able to have a point of reference to answer this question if they have not ridden in a Level 3 AV? Perhaps expert witnesses testifying as to a human being's natural state of complacency while utilizing AV features may become more and more common in criminal prosecutions surrounding negligent driving.

D. Society (and legislatures) must decide whether enforcement of traffic laws is necessary (and advantageous) as we advance from a Level 3 to a Level 5 fully automated driving world.

As technology in AVs and traffic enforcement improves, we must evaluate the impact officer discretion has had on the enforcement of traffic laws. No longer will police need to sit on the side of the road and wait for speeders. Speeding tickets can be automatically issued by electronic radar detections placed on polls and traffic signs. Parking tickets can be automatically issued by self-driving police cars or robots scouting the parking lot or cameras placed above. Red-light traffic cameras already take a car's

---

[210] Isidore, *supra* note 205.

[211] Amanda Cochran & Deven Clarke, *'No One was Driving the Car': 2 Men Dead After Fiery Tesla Crash Near The Woodlands Officials Say*, CLICK2HOUSTON.COM (Apr. 21, 2021), https://www.click2houston.com/news/local/2021/04/18/2-men-dead-after-fiery-tesla-crash-in-spring-officials-say/.

(and possibly driver's) picture and the license plate is captured so that an automated ticket is sent to the driver. We are looking at a scenario in which not hundreds but thousands upon thousands of traffic tickets can be issued electronically without any human oversight.

Will legislators view these automated sanction mechanisms differently in the future? Do we, as a society, want all traffic violations monitored and processed by cameras, sensors, and radars and issued daily? While an officer's discretion as to whether or not to issue the speeding ticket is certainly not perfect and can lead to abuse and racial profiling, are we comfortable with the plethora of traffic violations to come as cameras and artificial intelligence (AI) take over? If an AI's mission is to collect evidence and capture traffic and parking violators, rest assured, there will be no discretion (unless it is programmed to make certain exceptions).

Perhaps the thousands of tickets issued each day will create a revenue boon for many under-funded towns and cities. While legislators may want this increase in revenue, individual citizens may resent their bank, PayPal, or Venmo accounts being automatically infiltrated as the local government's AI traffic cop takes the traffic fine directly from the respective financial account associated with the driver/owner of the vehicle. Or, legislators can eliminate all strict liability traffic laws and only prosecute those that require a culpable mental state (negligent or reckless driving). This is a very real possibility as many of these traffic tickets for speeding, illegal parking, running red lights, etc. will be irrelevant as human drivers are replaced with Level 5 full automation. Level 5 AVs will presumably be programmed to obey traffic laws so most strict liability traffic laws such as speeding or running a red light would be irrelevant. Many police that spend their time enforcing traffic laws will be out of a job.

That said, we still currently need traffic enforcement and monitoring to keep the roads safe. The amount of AV crashes and negligent/reckless driving incidents make clear that AVs are like 16-year-old drivers learning to maneuver the roadways and identify pedestrians and objects on the road. And those behind the wheel are not paying enough attention to the road. AVs and their back-up drivers are not perfect and must be monitored.

IV. CONCLUSION

Some humans have indicated they want to live in a Level 5 fully automated driving world. According to consumer surveys, almost half of us would prefer to watch a movie, text, or sleep in the car rather than drive. In fact, some have already tricked a car in Autopilot and given up driving control to the car's artificial intelligence (despite manufacturer warnings). In a Level 5 world, there will be less pollution, less traffic congestion, and presumably, the roads will be safer. Humans, too tired or not interested in driving, will

soon forget how to drive and leave it up to the sensors, cameras, and LIDAR in the car to do it for them. GM already received a federal permit in 2018 to build Level 4 cars without steering wheels or pedals.[212]

Criminal liability in a Level 5 fully automated world where humans are simply passengers in the AV will shift to AV manufacturers. Criminal laws have not been designed to punish AVs with artificial intelligence, but rather, set forth punishments and penalties to ensure that unacceptable human behavior does not happen again. If the AV design is flawed, the programmers and manufacturers are at fault and may be held criminally liable. This would be similar to the criminal fault found in accidents involving driverless trains or airplanes being controlled on autopilot. Manufacturers will be punished based on their mental state and actions at the time the design flaw was created. Are manufacturers exhibiting a level of culpability similar to Ford's decision to not replace faulty gas tanks in Pintos or Volkswagen's deliberate attempt to manipulate emissions data? Human passengers/drivers inside the vehicle violating safety regulations set forth by AV manufacturers (ie, tricking Autopilot) may also be held criminally liable.

In today's age, human drivers in automated vehicles will be held criminally liable. However, a human driver in a Level 3 AV has a difficult task – he or she allows the AV to take over many of the driving functions but must also stay alert to the possibility that the AV may make a mistake and the driver may need to regain control. In a Level 3 AV, it is extremely easy for a criminal investigator to retrace a driver's steps and driving decisions before the crash. The amount of data collected will help the AV to improve, and it will also help prove the human driver was negligent.

The best compromise that can be made is to require law enforcement to obtain a warrant for all data in the hands of the car companies and on the EDR and continue to allow law enforcement to monitor the roads externally without any limitations (unless it is considered long-term monitoring). We also must assume that everything we do inside our cars will be observed by our car company (and with a warrant, a criminal investigator). Car companies are constantly collecting data to feed the AI.

Will Level 5 AVs become so commonplace "that the proverbial visitor from Mars might conclude they were an important feature of human anatomy"?[213] Perhaps they will not become an appendage like our smartphones, but our cars will certainly be watching us, listening to us, and

---

[212] Reuters Staff, *Cruise, GM to seek U.S. okay for self-driving vehicle without pedal, steering wheel*, REUTERS (Oct. 21, 2020), https://www.reuters.com/article/us-autonomous-cruise-nhtsa/cruise-gm-to-seek-u-s-okay-for-self-driving-vehicle-without-pedal-steering-wheel-idUSKBN2762SP.

[213] Riley v. California, 573 U.S. 373, 385 (2014).

learning from our past mistakes.[214]

[214] SAE, *supra* note 4 (According to BMW, "Vehicles of the future are becoming intelligent, high-tech devices, able to perceive and process more and more of their environment. With every newly-certified car, the fleet of connected components grows and the collective becomes more intelligent.").