WIRETAPS ON WHEELS

The Acceleration of Automotive Surveillance

EVAN ENZER
ANNA SIPEK
MAHIMA ARYA
NINA LOSHKAJIAN
DAVID SIFFERT
ELENI MANIS, PHD, MPA

NOV 1, 2022

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

Supported in part by a grant from the Open Society Foundations and by the John D. and Catherine T. MacArthur Foundation

EXECUTIVE SUMMARY

- New cars are surveillance on wheels, sending sensitive passenger data to carmakers and police. Cars also store enormous amounts of passenger data onboard, where police can extract it using specialized tools. We estimate that law enforcement agencies could have accessed car data hundreds of thousands of times in 2020.

- Constitutional loopholes allow access to most data on cars without a warrant. Police can access information from car-connected phones and online accounts without the warrant typically required.

- U.S. immigration agencies weaponize car data. Other law enforcement agencies are poised to follow suit if they are not already doing so.

- New legislation, enforcement of existing data protection laws, and responsible car design and data storage policies can shift car data surveillance into reverse.

I. INTRODUCTION

The cars we drive say a lot about us, but they see even more. Modern cars collect a huge amount of data, stored indefinitely onboard and in the cloud.[1] The data tracks not just the car, but its occupants: it records our location history, phone contents (contacts, emails, texts, tweets, social media feeds), voice recordings, weight, and other biometric data.[2] If this sounds creepily expansive, it is. Car data often is collected for the benefit of manufacturers, not drivers. Our information fuels a billion-dollar industry for subscription services as well as selling drivers' data to third parties, including law enforcement.[3] Many cars on the road feed this industry: 84 million connected cars beamed data to manufacturers and other companies in the U.S. in 2021.[4] Drivers can refuse some data collection, but saying "no" often comes at the cost of passenger safety: no data, no emergency roadside service or built-in navigation tools.[5]

For law enforcement, cars provide a rich and easily accessed source of surveillance data. Disturbingly, while cars collect much more detailed data than our cellphones, they receive fewer legal and technological protections, making them vulnerable to suspicionless searches. For instance, while the leading phone operating systems offer relatively robust cybersecurity features, most cars do not.[6] The overbroad automobile exception to the Fourth Amendment may allow law enforcement to search a car without a warrant.[7] A parallel Fourth Amendment exception for third-party data

---

[1] Cars generate 25 gigabytes of data per hour, and every year the average American spends 728 hours in a car. If you do the math, cars account for nearly 20 terabytes of data per year per person. Patrick Howell O'Neill, "Meet Berla, the Little-Known Company That Can Pull Smartphone Data from Your Car," CyberScoop, September 11, 2017, https://www.cyberscoop.com/berla-car-hacking-dhs/.

[2] See section entitled "what data is collected."

[3] Data Market in the Automotive Industry, 2022 - 27, Industry Share, Size, Growth," Mordor Intelligence, accessed April 15, 2022, https://www.mordorintelligence.com/industry-reports/big-data-market-in-the-automotive-industry. See Jeff Plungis, "Who Owns the Data Your Car Collects?," Consumer Reports, May 2, 2018, https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/.

[4] "Connected Car Fleet Worldwide by Region," Statista, September 2021, https://www.statista.com/statistics/1155517/global-connected-car-fleet-by-market/.

[5] For example, GM's OnStar privacy policy indicates that "some collection and sharing practices are tied to the products and services we offer. To stop the collection or sharing of some information, you may choose to decline those products and services or you may choose to accept limited functionality." *See* "Privacy Statement," OnStar Mobile Apps & OnStar Guardian App, accessed October 11, 2022, https://www.onstar.com/us/en/privacy_statement. *See also* Keith Barry, "Insurance Company Telematics Trade Perks for Privacy," *Wired*, August 19, 2011, https://www.wired.com/2011/08/insurance-company-telematics-trade-perks-for-privacy/..

[6] "Mobile Security & Privacy, Android Safety Center," Android, accessed September 27, 2022, https://www.android.com/safety/. Krista Rokform, "Apple Security Features On The IPhone 13," Rokform, January 20, 2020, https://www.rokform.com/blogs/rokform-blog/apple-security-features-on-the-iphone-13. "Mobile Operating System - an Overview," Science Direct, accessed September 27, 2022, https://www.sciencedirect.com/topics/computer-science/mobile-operating-system. Tim Roty, "Automotive Cyber Security and Encryption," *Medium* (blog), April 19, 2021, https://medium.com/@timroty/automotive-cyber-security-and-encryption-25c782f9a0a8.

[7] "Automobile Exception Law and Legal Definition," U.S. Legal, Inc., accessed April 18, 2022, https://definitions.uslegal.com/a/automobile-exception/.

suggests that once cars beam information to an automaker or insurer, drivers lose what few privacy protections they had.[8] Federal statutes provide few additional protections,[9] and just a few states have enacted middling measures to protect car data. As a result, law enforcement agencies can co-opt car data to explore the most vulnerable details of our lives, exposing protestors, people seeking reproductive healthcare or a safe home to police harassment or prosecution.

II. THREE KEY DATA COLLECTORS ON CARS

Modern cars generate data from innumerable sensors and onboard computers and pass that data to three key locations on a vehicle: the event data recorder, or "black box"; the telematics module, which is comparable to a modem with an associated hard drive; and the infotainment system, another hard drive where users' smartphone data is stored.

A. Black boxes

Event Data Recorders or "black boxes" are electronic devices that continuously monitor a vehicle so investigators can retrieve key information after an accident.[10] In 2012, 96% of all cars had a black box, and in 2015 Congress mandated them in all new automobiles.[11] Black boxes record data points from the moments before, during, and after an accident, including the state of the car pre- and post-crash, some of the driver's actions, the severity of the crash, whether seatbelts were used and whether airbags deployed.[12] Unlike the black boxes in airplanes, automotive black boxes do not record audio.[13] Data is stored locally on the box.[14]

---

[8] John Villasenor, "What You Need to Know about the Third-Party Doctrine," *The Atlantic*, December 30, 2013, https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/. *United States v. Miller*, 425 U.S. 435 (1976). *Smith v. Maryland*, 442 U.S. 735 (1979).

[9] In 2021, the U.S. Congress introduced but failed to pass a bipartisan bill, "The Closing Warrantless Digital Car Search Loophole Act," that would have barred warrantless searches of personal cars' computers. See Sam Biddle, "Bipartisan Bill Seeks to Stop Warrantless Car Spying by Police," The Intercept, November 18, 2021, https://theintercept.com/2021/11/18/bill-warrantless-searches-car-data-police/.

[10] Aaron Larson, "What is an Automobile Black Box" ExpertLaw, April 3, 2018, https://www.expertlaw.com/library/accidents/auto_black_boxes.html.

[11] "Car Black Box: Florida Event Data Recorder Rights in 2020," Fusco Law, February 22, 2020, http://www.fuscolaw.org/legal-tips/car-black-boxes-what-are-your-florida-privacy-rights-concerning-a-vehicle-event-data-recorder-in-2020/.

[12] "Event Data Recorder," National Highway Traffic Safety Administration, accessed April 12, 2022, https://www.nhtsa.gov/research-data/event-data-recorder.

[13] "What is a Car Black Box? 5 Things You Did Not Know," Kodsi Forensic Engineering Inc., July 8, 2021, https://kodsiengineering.com/what-is-a-black-box/.

[14] Larson, "Automobile Black Box."

Black boxes exist to collect a snapshot of information that reconstructs accidents, and as such, they have a limited storage capacity. A box stores no more than thirty seconds of data at a time and continuously overwrites its storage until an "event" occurs,[15] such as rapid deceleration.[16] From that point on, the box stops overwriting its memory and stores the final set of data points for recovery.[17]

Though black boxes collect vastly less information than telematics or infotainment systems, they have been around for much longer, and over time, they have received stronger protections than other sources of car data.

B. Telematics modules

Telematics modules are onboard modems that can transmit data collected by the vehicle to automakers, insurers, and telematics companies using a cellular or satellite connection.[18] A telematics system aggregates information from various sensors and systems built into vehicle. Together, these sensors describe the car's condition (vehicle faults, diagnostics, fuel consumption, and so on) and the driver, including their location data, data about driving habits (e.g., speed, nighttime driving), and biometric data, which depending on the system could include face measurements and images, voice recordings, and weight.[19] Telematics systems may also collect data from car-connected smartphones.[20]

There are two types of telematic systems—built-in modules and aftermarket additions—both with widespread adoption.[21] Original equipment manufacturer (OEM) telematics are increasingly included in vehicles by default. Some estimate that 50% to 60% of new cars sold globally in the past two years include this module, while others believe the number is up 80% to 90% for vehicles sold

---

15 Larson, "Automobile Black Box."

16 "Event Data Recorder (EDR)," *Squarell Technology*, accessed April 12, 2022, https://squarell.com/solutions/event-data-recorder-edr/.

17 "What Is a Black Box?," Kodsi Inc.

18 Aries, "What Is Telematics?" Verizon Connect, May 6, 2019, https://www.verizonconnect.com/resources/article/what-is-telematics/. Telematics systems also receive data for drivers, from directions to weather updates and emergency calls. Chris Bouchard, "Infotainment vs. Telematics Systems: What Is the Difference?," April 21, 2016, https://vin.dataonesoftware.com/vin_basics_blog/vehicle-infotainment-vs-telematics-systems-what-is-the-difference.

19 "Telematics Data," FleetGO , accessed April 12, 2022, https://fleetgo.com/kb/telematics/telematics-data/. Chris Burt, "New Biometric Vehicle Partnerships, Products and Concepts Unveiled for Payments, Personalization," Biometric Update, January 21, 2021, https://www.biometricupdate.com/202101/new-biometric-vehicle-partnerships-products-and-concepts-unveiled-for-payments-personalization.

20 Andrea Amico comments to the Surveillance Technology Oversight Project, September 26, 2022.

21 Jack Morse, "Your Car Knows Too Much about You. That Could Be a Privacy Nightmare," Mashable, September 18, 2021, https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect.

in the United States.[22] Over 80% of new cars globally will have OEM telematics by 2030.[23] Every major carmaker installs its own telematics module on new cars: GM OnStar, Toyota Connected Services, Nissan Connect, Ford SYNC, Mercedes "Mercedes me connect," and more. Vehicle owners, insurance companies, and fleet managers frequently install additional aftermarket telematics systems on vehicles to track their whereabouts and driver habits.

Deleting telematics data from cars is difficult to impossible for drivers. Vehicle sensor and telematic module data is accessible only to drivers who can and find it advisable to hack their cars. Moreover, telematics data is transmitted off cars to carmakers, insurers, and other companies in real-time or near real-time.[24] Most drivers have little control over what data is shared or how long it is stored. Of the top telematics companies, including Cambridge Mobile Telematics, Geotab, and GoFleet, most assert they can store data indefinitely and share it with whomever they wish.[25] Some insurers store telematic data for up to ten years.[26] By way of contrast, even Google, a favored source of law enforcement data, stores location data for 18 months.[27]

Drivers can avoid some data collection by refusing to use telematics services, but telematics providers force a choice.[28] Drivers can allow data collection and access telematics-enabled safety features, such as built-in navigation aids, insurance discounts, emergency services, and hands-free services, or they can refuse both.[29] Only a fraction of the collected data is needed to provide these

---

[22] For 50% estimate in 2022, see Alfred Ng, "What Your Car Knows About You," *POLITICO*, August 2, 2022, https://politi.co/3zQyxc7. For up to 62% estimate in 2020, *see* Martin Swegander, "The Global Automotive OEM Telematics Market" (Berg Insight, November 2021), https://www.berginsight.com/the-global-automotive-oem-telematics-market. For the up to 90% estimate, see Andrea Amico comments to the Surveillance Technology Oversight Project, September 26, 2022.

[23] Martin Swegander, "The Global Automotive OEM Telematics Market" (Berg Insight, November 2021), https://www.berginsight.com/the-global-automotive-oem-telematics-market. Ng, "What Your Car Knows."

[24] Aries, "What Is Telematics?".

[25] "Privacy Policy," Geotab. "Privacy Policy," GoFleet. "Description of Processing of Personal Data," Verizon, accessed May 12, 2022, https://www.verizon.com/about/privacy/description-processing-personal-data-verizon-connect. "Privacy Policy," Cambridge Mobile Telematics, accessed July 6, 2022, https://www.cmtelematics.com/privacy-policy/. Martin, "Connected Cars Worldwide."

[26] Kaveh Waddell, "What You're Giving Up When You Let Your Car Insurer Track You In Exchange for Discounts," Consumer Reports, October 7, 221AD, https://www.consumerreports.org/car-insurance/how-car-insurance-telematics-discounts-really-work-a1549580662/.

[27] Waddell, "What You're Giving Up."

[28] Barry, "Insurance Company Telematics."

[29] SiriusXM and Progressive provide representative examples. "Privacy Policy," SiriusXM Connected Vehicle Services, accessed October 11, 2022, https://www.siriusxmcvs.com/privacy-policy/. "Snapshot Terms & Conditions," Progressive. "Privacy Statement," OnStar Mobile Apps & OnStar Guardian App.
Dave LaChance, "U.K. Study Finds 17% of Young Drivers Concerned about Security of Telematics Data," *Repairer Driven News*, April 28, 2022, https://www.repairerdrivennews.com/2022/04/28/u-k-study-finds-17-of-young-drivers-concerned-about-security-of-telematics-data/.

services: giving emergency roadside help, for example, requires knowing where a driver is now, not where they have been in the past or what their favorite destinations are.

C. Infotainment systems

Infotainment systems yield the most sensitive locally stored car data. Telematics and infotainment systems frequently share the same user interface screen and share some functions, such as navigation.[30] But as the name suggests, infotainment systems add entertainment to cars, playing music and videos, allowing calls and texts (not just emergency communications), and allowing drivers and passengers to access their smartphones' functions through their cars.[31] Consumer Reports and IHS Markit report that 98% of new vehicles include at least one infotainment interface.[32]

From a surveillance perspective, infotainment systems are anything but fun, turning constitutionally protected phone data into vehicle data that may be searchable without a warrant. A car's infotainment system stores highly personal data from smartphones and other mobile devices that connect to the system with USB cables or Bluetooth.[33] If you use your infotainment system to text, make a call, send email, check social media or browse the web, the system stores the content and data associated with those actions on the car.[34] Anyone who uses an infotainment system to access the car's built-in apps, such as navigation services, shares their location history, voice commands, and any passwords they use with the car.[35] The resulting data is stored on the car's infotainment system and shared with vehicle manufacturers, rental companies, infotainment providers, and app companies in accordance with their business policies.[36]

---

[30] Bouchard, "Infotainment vs. Telematics Systems."

[31] Tiff Rossi, "A Brief History of In-Vehicle Infotainment and Car Data Storage," Tuxera, July 19, 2021, https://www.tuxera.com/ja/blog/a-brief-history-of-in-vehicle-infotainment-how-tuxera-fits-in/.

[32] Keith Barry, "Screen Stars: Which Infotainment System Deserves a Leading Role in Your Next Car?," Consumer Reports, accessed August 5, 2020, https://www.consumerreports.org/infotainment-systems/screen-stars-in-car-infotainment-systems/.

[33] Robert S. Kinder "Infotainment Systems: What's in Your Car & How Is It Used?" DJS Associates, October 9, 2017. https://www.forensicdjs.com/blog/infotainment-systems-whats-car-used/.

[34] Kinder, "Infotainment Systems." See Olivia Solon, "Insecure Wheels: Police Turn to Car Data to Destroy Suspects' Alibis," NBC News, December 28, 2020, https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939.

[35] "Infotainment System Data Retrieval," North Eastern Technical Services, accessed April 12, 2022, https://www.northeasterntechnical.com/infotainment-system-data-retrieval. Matt McFarland, "Your Car Knows Secrets about You. Here's How to Protect Yourself," CNN, May 18, 2020, https://www.cnn.com/2020/05/18/tech/car-data-safety/index.html.

[36] "Connected Cars: What Happens to Our Data on Rental Cars?," Privacy International, accessed April 12, 2022, https://www.privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf.

Like telematics systems, infotainment systems come in two varieties: OEM systems installed by carmakers on the assembly line, and add-ons that integrate smartphones into a car's infotainment system. There are three notable smartphone integration firms: MirrorLink, Apple CarPlay, and Android Auto. The oldest system, MirrorLink, was developed by Nokia and provides software that carmakers can modify to connect smartphones to their cars.[37] Starting in 2014 and 2015, Apple CarPlay for iOS devices and Google's Android Auto for Android devices introduced proprietary systems that link smartphones to cars. In 2020, 76% of new cars were compatible with Apple CarPlay and 69% with Android Auto.[38] From a surveillance perspective, these big tech middlemen add another layer of data sharing to the infotainment enterprise, making the information even more accessible to law enforcement.

As is the case with telematics data, drivers can attempt to delete sensitive data from an infotainment system. However, most systems do not delete car data fully: deep in system memory, infotainment systems continue to store sensitive personal and identifying information.[39] Even resetting an infotainment system to its factory default settings may not delete anything until new data overwrites the system's previous contents.[40]

D. Other data sources (*e.g.*, biometric monitors, cameras, autonomous driving systems)

Cars are full of processors that generate data—and pass it to the systems already mentioned. Some cars contain computers that operate cameras, enable autonomous driving, or perform biometric monitoring, generating corresponding data.[41] On-car data retention for these processors varies depending on the car's make and model and the computer's function. All of this data, insofar as it is needed (or wanted) by carmakers or insurers, passes through the telematics module—the car's "modem"—on its way off the car and can be considered part of the broader telematics infrastructure. Any stored information that does not touch telematics is either stored by the infotainment system, the black box, or substantially similar computer memory.

---

[37] Chris Rosamond, "What Is MirrorLink?," *Auto Express*, December 16, 2020, https://www.autoexpress.co.uk/car-news/99194/what-is-mirrorlink-guide-to-the-car-smartphone-hook-up-system. "MirrorLink," accessed September 7, 2022, https://mirrorlink.com/phones.

[38] Barry, "Screen Stars."

[39] Thomas Brewster, "Feds Can Dig Up 'Deleted' Location Data From Your Car Entertainment System," Forbes, accessed April 12, 2022, https://www.forbes.com/sites/thomasbrewster/2018/10/17/feds-are-digging-up-deleted-location-data-from-car-entertainment-systems/.

[40] "How Infotainment Systems Work and How They Record Data," Kodsi Engineering Inc., June 3, 2021, https://kodsiengineering.com/infotainment-systems/.

[41] Albert Amos and Robert Bosch, "Comparison of Event-Triggered and Time-Triggered Concepts with Regard to Distributed Control Systems," GmbH Embedded World, 2004, Nürnberg, 236.

III. HOW LAW ENFORCEMENT ACCESSES CAR DATA

Automobiles offer law enforcement a carload of personal data: location data, smartphone data, even biometric data—often without the need for a warrant.

A. Car data on company servers

The easiest way for law enforcement to obtain car data is simply to ask for it.[42] Telematic systems communicate a range of vehicle and driver information to carmakers, insurers, and telematics companies' remote corporate servers, and companies freely admit to sharing clients' data with law enforcement. For example:

- General Motors OnStar shares customers' location data and audio and video recordings with law enforcement agencies without a subpoena or warrant requirement.[43]
- Allstate offers discounts to drivers in exchange for their telematics data,[44] and shares this data with law enforcement agencies without a subpoena or warrant requirement.[45]
- FCA, the telematics and infotainment provider for Chrysler, Dodge and Jeep, and others shares users' data with law enforcement agencies, without a subpoena or warrant requirement—and indeed, sometimes simply in response to "request[s], whether formal and informal, from law enforcement or a government authority."[46]

Surveillance systems are opaque, and law enforcement's access to telematics data is particularly inscrutable. Most carmakers do not disclose requests for vehicle data. By deciding to withhold

---

[42] National Security Letters permit law enforcement to compel records with little oversight. "National Security Letter," Legal Information Institute, accessed April 15, 2022, https://www.law.cornell.edu/wex/national_security_letter.

[43] See "Privacy Statement," OnStar Mobile Apps & OnStar Guardian App, accessed October 15, 2022, https://www.onstar.com/content/tcps/us/20180501_7012021/privacy_statement.html. GM explains that it may share customers' OnStar data "As required or permitted by law, such as in conjunction with a subpoena, government inquiry, litigation, dispute resolution, or similar legal process, when we believe in good faith that disclosure is necessary to protect our rights, your safety, or the safety of others, to detect, investigate and prevent fraud, or to conduct screening to ensure you are not on any government list of restricted parties." GM does stipulate that "We generally do not release those records (including audio records) [associated with a crash or other "service" event] unless we receive an appropriate court order or are otherwise required by applicable law."

[44] "Drive Safe & Earn with Drivewise" Allstate, accessed September 15, 2022, https://www.allstate.com/drivewise.

[45] Allstate may not require even a subpoena to share customer data with law enforcement. About sharing with "Law enforcement, regulators and other parties for legal reasons," it indicates "Personal information may be disclosed to third parties, as required by law or subpoena, or if we reasonably believe such action is necessary to: comply with the law and the reasonable requests of regulators, law enforcement or other public authorities, protect our or others safety, rights or property, and investigate fraud or to protect the security or integrity of our Sites or any product or services." *See* "Privacy Policy," Allstate, accessed October 13, 2022, https://www.allstate.com/about/privacy-statement-aic.aspx.

[46] "Uconnect and SiriusXM Guardian - Privacy Policy," Chrysler, accessed September 25, 2022, https://www.driveuconnect.com/connectedservices/privacy.html. SiriusXM serves over 15 OEM programs. "About," SiriusXM Connected Vehicle Services, accessed September 27, 2022, https://www.siriusxmcvs.com/about/.

transparency reports, which are standard for many consumer-facing companies,[47] vehicle makers, insurers, and others intentionally hide how many government requests they receive each year. This level of secrecy is all too common for government surveillance. U.S. police are notoriously secretive and often hide any information necessary for even minimal public oversight.[48]

Rideshare firms, which disclose the number of police requests they receive for data comparable to telematics, are the closest proxy available to illustrate the potentially astronomic scope of vehicle data surveillance.[49] Uber received nearly 5000 law enforcement requests in 2020; Lyft received slightly over 2000.[50] Together, the companies had about two million cars on the road in 2020.[51] There were roughly 84 million connected cars on the road in 2021,[52] meaning that car manufacturers, telematics companies, and insurers collected data on over 40 times more cars than Uber and Lyft. If manufacturers, telematics, and insurers received a proportional number of law enforcement requests for car data, these companies would have received over 280,000 law enforcement requests in 2020.[53] If this reasonable estimate is even roughly accurate, it is staggering: by point of comparison, Google reported receiving under 80,000 law enforcement requests for user data in the U.S. in 2020.[54] If law enforcement requests to car companies have not reached these levels to date, it is a reflection that police departments have been slow to realize the overwhelming

---

[47] Most of the large consumer internet companies publish transparency reports. Spandana Singh and Leila Doty, "The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules," New America, December 9, 2021, http://newamerica.org/oti/reports/transparency-report-tracking-tool/.

[48] "Police Secrecy, The Record," The Marshall Project, accessed September 27, 2022, https://www.themarshallproject.org/records/2460-police-secrecy. NYPD refuses to release information about its surveillance of Black Lives Matter protestors. "USA: NYPD Ordered to Hand over Documents Detailing Surveillance of Black Lives Matter Protests Following Lawsuit," Amnesty International, August 1, 2022, https://www.amnesty.org/en/latest/news/2022/08/usa-nypd-black-lives-matter-protests-surveilliance/.

[49] "Legal," accessed September 27, 2022, https://www.uber.com/legal/en/document/?name=privacy-notice&country=united-states&lang=en. "Lyft Privacy Policy," June 30, 2021, https://www.lyft.com/privacy.

[50] "Uber," accessed May 2, 2022, https://www.uber.com/us/en/about/reports/transparency/law-enforcement/. "Lyft's Law Enforcement Support" Lyft. Looking beyond law enforcement requests to regulatory requests, the number affected users reaches well into tens of millions for Uber alone. "Uber Transparency Report," Uber, accessed May 2, 2022, https://www.uber.com/us/en/about/reports/transparency/regulatory/.

[51] Melissa Berry, "How Many Uber Drivers Are There in 2022?," *The Rideshare Guy Blog and Podcast* (blog), May 1, 2022, https://therideshareguy.com/how-many-uber-drivers-are-there/.

[52] "Connected Car Fleet," Statista.

[53] This estimate was reviewed and approved by Andrea Amico, an expert in the fields of privacy, automobiles, and criminal procedure. However, it is only a projection of the possible number of requests. The actual number is dependent on police practices that are unknown at the time of drafting. Amico points out that law enforcement can also request car data from hundreds of third-party car data brokers, such as Otonomo, which holds location data from 50 million cars worldwide. *See* Joseph Cox, "Class-Action Lawsuit."

[54] "Requests for User Information – Google Transparency Report," Google, accessed September 15, 2022, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period.

amount of personal information made available to them via automobiles; and a warning that lawmakers and vehicle manufacturers should act before police departments do.

B. Physical retrieval of data stored on the car

For dragnet searches, law enforcement can't beat car companies' server data: officers can demand data for everyone who drove to a protest, an abortion clinic, or across the U.S. border in a stretch of time. But if police have physical access to a car and want to know about its passengers, they needn't only ask car companies for data. They can break into a car's hard drives and access locally stored information with tools designed specifically for law enforcement.

Black box data

Police routinely retrieve black box data.[55] Texas police, for example, downloaded black box data two thirds of the time in fatal or possibly fatal crashes.[56] To access the data on black boxes, police plug a device—typically Bosch's Crash Data Retrieval tool—into a port usually located under the steering wheel.[57] Bosch's device works on over 90% of models year from 2016 and later.[58] The other 10% are covered by other event data retrieval tools.[59] After recognizing the retrieval device, a car's black box generates a report[60] that gives law enforcement information about the vehicle's speed, braking, and acceleration.[61]

Telematics, infotainment, and other computer systems

Since 2013, law enforcement agencies have been able to extract cars' telematics and infotainment data using Berla's Project iVe device.[62] When physically connected to a car, the device downloads a forensic copy of both the telematics and infotainment systems.[63] Berla's May 2022 agreement with Customs and Border Protection (CBP) promises car data, including "geo-positioning data (*i.e.*,

---

[55] Adam M. Gershowitz, "The Tesla Meets the Fourth Amendment," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, October 29, 2021), https://doi.org/10.2139/ssrn.3958465.

[56] Gershowitz, "Tesla Meets the Fourth."

[57] "EDR Q and A," National Traffic Safety Administration, 1, accessed September 7, 2022, https://www.nhtsa.gov/sites/nhtsa.gov/files/fmvss/EDR_Qas_11Aug2006.pdf. Gershowitz, "Tesla Meets the Fourth."

[58] "State of EDR in the US CDR Update June 2022," Ruth Consulting, June 2022, https://iptm.unf.edu/uploadedFiles/symposium/handouts/Ruth-USEDRStatus06032022.pdf.

[59] "State of EDR in the US," Ruth Consulting.

[60] "The Bosch CDR Tool," Crash Data Group, accessed June 27, 2022, https://crashdatagroup.com/pages/the-bosch-cdr-tool.

[61] ""Black Box 101: Event Data Recorders," Consumer Reports, accessed September 7, 2022, https://www.consumerreports.org/cro/2012/10/black-box-101-understanding-event-data-recorders/index.htm.

[62] O'Neill, "Meet Berla."

[63] O'Neill, "Meet Berla."

navigation history, recent destinations, & favorite locations), call logs, contact lists, SMS messages, emails, pictures, videos and social media feeds."[64] CBP's vendor also describes Berla devices' ability to extract data that predicts drivers' "future plan[s]" and "known associates and [can] establish communication patterns between them."[65]

Berla's technology appears to be frighteningly successful at breaking into cars and relatively easy to use. According to its maker, the device can successfully download data from the vast majority of American and European cars.[66] Users can store and access car data on the Berla mobile app or computer software.[67] Berla partners with the cellphone data extraction firm Cellebrite to optimize data to be imported to existing police databases.[68] The company hopes to eventually eliminate the need for a physical data extraction device: it aims to "build native infotainment apps to collect, store, and forward data,"[69] repurposing a car's infotainment and telematics systems for spying.

IV. HARMS

Harms associated with cars' location data

Car location data may be even more accurate than location data derived from cellphones and other mobile devices.[70] The Supreme Court famously held that cellphones deserve constitutional protections because they convey an "ever-alert," "nearly infallible," "all-encompassing record" of a person's "familial, political, professional, religious, and sexual associations."[71] There is no reason car data should be more accessible to police.

---

[64] Department of Homeland Security Customs & Border Protection (CBP), "Statement of Work: Berla Vehicle Forensic Kit Acquisition, License Renewals, and Training," May 19, 2022, https://www.highergov.com/document/70b06c22q00000120-attachment-b-statement-of-work-pdf-24e2da/.

[65] Sam Biddle, "Your Car Is Spying on You, and a CBP Contract Shows the Risks," *The Intercept*, May 3, 2021, https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/.

[66] DHS Science and Technology Directorate, 2016 R&D Showcase: Project IVe: Forensics for Vehicle Infotainment and Navigation Systems, 2016, https://www.youtube.com/watch?v=E0DQEVgJY5k.

[67] "Products," Berla Co., accessed April 15, 2022, https://berla.co/ecosystem/.

[68] "Products," Berla Co. "Cellebrite Inspector Provides Berla Ive Support," Cellebrite, September 5, 2019, https://cellebrite.com/en/cellebrite-inspector-provides-berla-ive-support/.

[69] DHS Science and Technology Directorate.

[70] Alfred Ng, "What Your Car Knows about You," POLITICO, August 2, 2022, https://politi.co/3zQyxc7.

[71] *Carpenter v. United States*, 585 U.S. ___ (2018), https://supreme.justia.com/cases/federal/us/585/16-402/. This case concerns cell-site location information, but the reasoning is applicable to other forms of location data. *In Re Search of Info. Stored At Premises Controlled By Google*, 481 F. Supp. 3d 730 (N.D. Ill 2020). https://casetext.com/case/in-re-search-of-info-stored-at-premises-controlled-by-google.

Law enforcement misuses cars' location data in two distinct ways. First, law enforcement agencies readily admit that they track the location of cars associated with persons of interest.[72] What they fail to emphasize is that Black and Indigenous People of Color (BIPOC people), immigrants, people seeking abortions, lawful protestors, Muslims, and LGBTQ+ individuals are all "persons of interest" to American police. Even as biased surveillance abuses grow, courts and legislatures have failed to keep up and constrain these tracking abuses.

In addition to targeting particular cars' location data, law enforcement officers regularly serve geofence warrants that force Google and other tech firms to identify individuals in a particular area at a particular time.[73] These digital dragnets can reveal the locations of hundreds or thousands of people with no suspicion of wrongdoing.[74] Police have used these searches to identify those present at political events,[75] including Black Lives Matter protests.[76] When used to investigate crimes, geofence warrants have led to false arrests, among them a bicyclist whose training route circled a crime scene and an Arizona man falsely accused of murder.[77]

There's no reason to think that geofence warrants stop or will stop with tech giants like Google. Police already send geofence requests to rideshare companies Uber and Lyft.[78] Car manufacturers, telematics companies, insurers, and their third parties (e.g. data brokers like Otonomo and Wejo) store detailed location data for vehicle tracking, service provision, marketing, and insurance purposes[79]—and may be friendlier to law enforcement causes than tech companies, who are under

---

[72] For an example, see Kate Cox, "No, Cops Aren't Using SiriusXM to Find Criminals. Here's How They Do It," *Ars Technica*, January 8, 2020, https://arstechnica.com/tech-policy/2020/01/no-cops-arent-using-siriusxm-to-find-criminals-heres-how-they-do-it/.

[73] Leila Barghouty, "What Are Geofence Warrants?," The Markup, September 1, 2020, https://themarkup.org/the-breakdown/2020/09/01/geofence-police-warrants-smartphone-location-data.

[74] Barghouty, "What Are Geofence Warrants?"

[75] "Search Warrant no. 1700264," Superior Court of California, Alameda County, 2017, https://www.documentcloud.org/documents/6935331-UCB-Search-Warrant.html. J. Fingas, "Minneapolis Police Used Google Location Data to Find George Floyd Protesters," Engadget, February 17, 2021, https://www.engadget.com/police-get-google-location-data-george-floyd-protests-183114536.html.

[76] Corin Faife, "FBI Used Geofence Warrant in Seattle after BLM Protest Attack, New Documents Show," *The Verg*, February 5, 2022, https://www.theverge.com/2022/2/5/22918487/fbi-geofence-seattle-blm-protest-police-guild-attack.

[77] Kim Lyons, "Google Location Data Turned a Random Biker into a Burglary Suspect," *The Verge*, March 7, 2020, https://www.theverge.com/2020/3/7/21169533/florida-google-runkeeper-geofence-police-privacy. See Meg O'Connor, "Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder," *Phoenix New Times*, Jan. 16, 2020, https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374.

[78] Sidney Fussell, "An Explosion in Geofence Warrants Threatens Privacy Across the US," *Wired*, August 27, 2021, https://www.wired.com/story/geofence-warrants-google/. Albert Fox Cahn, "This Unsettling Practice Turns Your Phone into a Tracking Device for the Government," Fast Company, January 17, 2020, https://www.fastcompany.com/90452990/this-unsettling-practice-turns-your-phone-into-a-tracking-device-for-the-government.

[79] "Privacy Statement" General Motors." "Privacy Policy," Ford Motor Company. "Legal Privacy Policy," Nissan USA, accessed August 30, 2022, https://www.nissanusa.com/privacy.html. Waddel, "What You're Giving Up."

pressure to stop policing customers.[80] Car-based location data held by companies could easily reveal vehicles present at particular locations and specified times, where those cars started and ended the day, and vehicles that drove along particular routes. As states criminalize abortion in the wake of the *Dobbs v. Jackson Women's Health Organization* ruling, we can expect prosecutors to demand automobile location data that criminalizes people seeking and providing reproductive care—including, for example, motorist information for every car that drove from abortion restrictive Indiana to reproductive healthcare clinics in Michigan. Given Immigration and Customs Enforcement's documented use of location and license plate data to track cars,[81] its recent purchase of Berla devices,[82] and its new contract to equip immigrants with location-tracking cellphones,[83] it would be surprising if the agency is not yet routinely demanding that companies yield car data to track people moving across the U.S. border.[84]

Even municipal governments collect residents' trip data en masse, suggesting that they may also tap car data for dragnet searches.[85] The Los Angeles Department of Transportation's (LADOT) maintains one of the largest programs of this sort.[86] Los Angeles tracks thousands of bikes and scooters available for public rental.[87] Every one of these vehicles reports its precise location to local government agencies.[88] Police would normally require a warrant to obtain this information under state law, but LADOT does no such thing, according to federal courts.[89] New York City's contactless payment program for subways and buses tracks public transit riders in a similar fashion.[90]

---

[80] "Geofence Letter," S.T.O.P. - The Surveillance Technology Oversight Project, December 8, 2020, https://www.stopspying.org/geofence-letter.

[81] Brewster, "These Companies Track Millions of Cars."

[82] Biddle, "Your Car Is Spying."

[83] Caroline Haskins, "ICE Spends $7.2 Million to Increase Facial Recognition and Location Tracking of Migrants," Business Insider, May 2, 2022, https://www.businessinsider.com/ice-7-million-contract-trust-stamp-facial-recognition-location-tracking-2022-5.

[84] Branko Marcetic, "ICE Doesn't Need a Warrant to Spy on You," Jacobin, July 26, 2022, https://jacobin.com/2022/07/ice-dhs-homeland-security-tech-selling-data-geolocations-spying.

[85] Jaqui Irwin and Buffy Wicks, "Local Transportation Agencies Are Tracking E-Bikes and e-Scooters: They Aren't Big Brother," *CalMatters*, July 28, 2020, http://calmatters.org/commentary/my-turn/2020/07/local-transportation-agencies-are-tracking-e-bikes-and-e-scooters-they-arent-big-brother/.

[86] Los Angeles Department of Transportation (LADOT), "Strategic Implementation Plan." June 2018. https://static1.squarespace.com/static/57c864609f74567457be9b71/t/5b625117575d1f924b6570ad/1533169956703/LADOT_SIP_06122018.pdf.

[87] LADOT, "Strategic Implementation Plan."

[88] LADOT, "Strategic Implementation Plan."

[89] Irwin and Wicks, "Transportation Agencies Are Tracking E-Bikes." James Orenstein, "Administrative Requirement for E-Scooter Location Records Not a Fourth Amendment Search," ZwillGen, June 3, 2022, https://www.zwillgen.com/law-enforcement/electric-scooter-location-records-not-a-fourth-amendment-search/.

[90] The Surveillance Technology Oversight Project (S.T.O.P.), "OMNY Searches Oh MY," October 1, 2019, https://www.stopspying.org/omny.

Law enforcement agencies and prosecutors can also simply purchase location data from willing sellers. The market for cellphone location data, license-plate reader data, and vehicle locator systems demonstrate law enforcement's appetite for buying data they cannot legally (or easily) collect or compel companies to share.[91] Until its practices were exposed in May 2022, data brokerage SafeGraph sold abortion clinic visitors' location data, apparently sourced in part from internet-connected vehicles.[92] The data was available for anti-abortion groups to purchase, as well as to government agencies gearing up to prosecute abortion-seekers and people helping them (it included data that could reveal patients' states of origin and out-of-state hosts).[93] Another company, Otonomo, analyzes telematics data from tens of millions of vehicles and targets government clients with so-called "smart city" solutions.[94] It faces a class-action law suit for violating California drivers' privacy rights under the California Invasion of Privacy Act.[95] Yet another company, Ulysses, collects real-time vehicle location data with plans to sell this information to the military.[96] Data brokers have discovered car-based data as a rich source of location data, and it is on the table as a new surveillance source.

Harms associated with communications captured by cars

U.S. law enforcement agencies routinely spy on Americans' communications in real-time and in retrospect. Car data is being tapped for both purposes: officers "bug" cars using telematics modules and hack infotainment systems to retrieve communications records comparable to those found on smartphones.

---

[91] Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, "Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers," December 9, 2021, https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/.

[92] Joseph Cox, "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics," *Vice*, May 3, 2022, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[93] Matthew Gault, "The Data Broker Tracking Abortion Clinic Visits Is Also Selling to the CDC." May 4, 2022, https://www.vice.com/en/article/m7vzab/the-data-broker-tracking-abortion-clinic-visits-is-also-selling-to-the-cdc.

[94] "Otonomo-Presentation," accessed August 30, 2022, https://www.documentcloud.org/documents/20515641-otonomo-presentation. "Connected Car Data for Smart Cities: Get Richer Vehicle Datasets," Otonomo, accessed September 16, 2022, https://otonomo.io/use-cases/smart-cities-car-data/.

[95] Joseph Cox, "Class-Action Lawsuit Targets Company That Harvests Location Data from 50 Million Cars," *Vice* (blog), April 15, 2022, https://www.vice.com/en/article/y3v95k/car-location-data-otonomo-class-action-lawsuit.

[96] Joseph Cox, "Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military," *Vice*, March 17, 2021, https://www.vice.com/en/article/k7adn9/car-location-data-telematics-us-military-ulysses-group.

Law enforcement agencies listen to conversations happening in cars using cars' emergency response systems and hands-free microphones, a process colloquially called "cartapping."[97] In one case, a court ordered a telematics company to let the FBI listen into a car using its emergency assistance system.[98] The company complied for 30 days before stopping. That wasn't enough for the FBI, who complained that the company was in contempt of court.[99]

Police also raid infotainment systems when they cannot technologically or legally access communications data from smartphones or other sources.[100] California police used this tactic to access phone data after Apple refused their request to break into an iPhone.[101] As Berla's CEO said, "[t]he cellphone's locked and you can't get in it, but they've connected the phone to the car, so it reveals some data about the phone."[102] "Some data" is an understatement: cars store text messages, phone records, contact lists, in-car conversations, and social media feeds, creating a record of drivers' thoughts, behaviors, and personal, professional, religious, and political commitments and associations.[103]

What's more, a single rental car can yield much more information than a single smartphone. One rental car in a Baltimore airport yielded personal data from 70 users who had plugged their phones into the car,[104] including, according to Berla's founder, "[a]ll of their call logs, their contacts, and their SMS history, as well as their music preferences… some of their Facebook and Twitter things as well."[105] When rental car companies fail to delete customers' phone data from rental cars they return (a routine practice that is subject to at least one class-action lawsuit[106]), they make customers'

---

[97] Susan Brenner, "Can You Trust Your Car? – Part 2," *CYB3RCRIM3* (blog), March 9, 2009, https://cyb3rcrim3.blogspot.com/2009/03/can-you-trust-your-car-part-2.html. Thomas Brewster, "Cartapping: How Feds Have Spied On Connected Cars For 15 Years," *Forbes*, January 15, 2017, https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/.

[98] Brewster, "Cartapping."

[99] Brewster, "Cartapping."

[100] George L. Seffers, "DHS Navigates the World of Vehicular Digital Forensics," *SIGNAL Magazine*, May 24, 2016, https://www.afcea.org/content/Article-dhs-navigates-world-vehicular-digital-forensics.

[101] O'Niel, "Meet Berla."

[102] Seffers, "DHS Navigates.

[103] Moritz Büchi, Noemi Festic, and Michael Latzer, "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda," *Big Data & Society* 9, no. 1 (January 1, 2022): 20539517211065370, https://doi.org/10.1177/20539517211065368.

[104] Riley Beggin, "Questions Arise Over Police Searches of Car Data Systems," GovTech, January 4, 2022, https://www.govtech.com/public-safety/questions-arise-over-police-searches-of-car-data-systems.

[105] Gershowitz, "Tesla Meets the Fourth.""

[106] Laura Pennington, "Avis Class Action Says In-Car Technology Stores Customer Data," Top Class Actions, January 7, 2019, https://topclassactions.com/lawsuit-settlements/privacy/avis-class-action-says-car-technology-stores-customer-data/.

phone data available to future renters and to law enforcement agencies or prosecutors who may search the car for totally unrelated purposes months or years later. Law enforcement calls car-breaking "digital vehicle forensics."[107] In truth, it is violative surveillance that sidesteps legal protections on smartphone data for anyone who connects their phone to an infotainment system.

Harms associated with cars' biometric data

Cars with telematics and infotainment systems collect source material for sensitive biometric data: photos that can be fed into facial recognition software; voice commands that can produce a driver's voiceprint. A few cars already include built-in biometric tools, like a fingerprint scanner on some 2022 Mercedes.[108] Other tools aim to verify drivers' identities with facial recognition,[109] scan for distraction,[110] and to measure energy levels and intoxication.[111] Already enacted federal legislation may make implementing more of these biometric monitoring systems mandatory within the next decade.[112]

Biometric technologies range from invasive to completely bogus. Worse yet, BIPOC people and people with disabilities—two groups already at risk of dangerous interactions with the police—suffer disproportionately from their mistakes and malfunctions.

Consider facial recognition, an error-prone tool that uses facial geometry to identify individuals. Facial recognition disproportionately misidentifies BIPOC people, women, young, and elderly

---

[107] Olivia Solon, "Insecure Wheels: Police Turn to Car Data to Destroy Suspects' Alibis," NBC News, December 28, 2020, https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939.

[108] "Customized for Either the Mr or Mrs, the W206 Mercedes-Benz C-Class Offers a Fingerprint Scanner," WapCar News, March 1, 2022, https://www.wapcar.my/news/customized-for-either-the-mr-or-mrs-the-w206-mercedesbenz-cclass-offers-a-fingerprint-scanner-41902.

[109] Jonathan Bilyk, "Class Action: Subaru DriverFocus System Improperly Scans Driver's Faces, Eyes," *Cook County Record*, accessed September 27, 2022, https://cookcountyrecord.com/stories/613746211-class-action-subaru-driverfocus-system-improperly-scans-driver-s-faces-eyes.

[110] Chris Burt, "Automotive Biometrics Market Sizzles but Faces Familiar Demographic Disparity Challenge," Biometric Update, April 23, 2021, https://www.biometricupdate.com/202104/automotive-biometrics-market-sizzles-but-faces-familiar-demographic-disparity-challenge. greentheonly, *Tesla Driver Monitor System Outputs at Night (Uncut)*, 2021, https://www.youtube.com/watch?v=vTCbBsMJ3ts.

[111] Burt, "Automotive Biometrics Market Sizzles." Xavier Boucherat, "In-Cabin Monitoring: The Future Interface of Mobility?," *Automotive World*, May 27, 2021, https://www.automotiveworld.com/articles/in-cabin-monitoring-the-future-interface-of-mobility/.

[112] Pub. L. 117—58 § 24220 (2021). The Safeguarding Privacy In Your Car Act of 2022, S. 4647, 117th Cong. 2d. Session (2022) would repeal this provision.

people.[113] It struggles to identify at all anyone in poor quality images.[114] Facial recognition in cars—so-called "driver authorization" tools—could lock BIPOC drivers out of their own vehicles.[115]

Other biometric tools for cars, like attention-tracking and emotion-analyzing software, make bogus assumptions about what face and body movements convey about a person's internal state.[116] Attention-monitoring software has flagged students with disabilities—and students who simply look away from their screens—as cheaters.[117] Emotion-analyzing tools, based on junk science, penalize women for their speech patterns and Black people for normal facial expressions.[118] Bogus biometric software could wrongly flag people for careless or tired driving, with dangerous consequences on the road.[119]

V. LEGALITY

Law enforcement agencies can perpetrate these harms because they have easy, legal access to car data.

A. Constitutional law

The Bad News…

Cars have emerged through decades of cases as an exception to the protections Americans normally have against searches and seizures. As part of a systematic, decades-long attempt to undermine the Fourth Amendment,[120] the Supreme Court has held that law enforcement officials do not need a warrant before searching a vehicle as long as they have probable cause.[121] The court resolved during

---

[113] Eleni Manis et al., "Scan City: A Decade of NYPD Facial Recognition Abuse" (Surveillance Technology Oversight Project (S.T.O.P.), July 8, 2021), https://www.stopspying.org/scan-city.

[114] Eleni Manis et al., "Scan City."

[115] Burt, "Automotive Biometrics Market Sizzles."

[116] Lisa Feldman Barrett et al., "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," *Psychological Science in the Public Interest*, July 17, 2019, https://doi.org/10.1177/1529100619832930; Jay Stanley, "The Dawn of Robot Surveillance," American Civil Liberties Union, 2019, https://www.aclu.org/report/dawn-robot-surveillance.

[117] Drew Haewell, "Cheating-Detection Companies Made Millions during the Pandemic. Now Students Are Fighting Back.," *Washington Post*, November 12, 2020, https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/.

[118] Kate Crawford, "Artificial Intelligence Is Misreading Human Emotion," *The Atlantic*, April 27, 2021, https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.

[119] Burt, "Automotive Biometrics Market Sizzles."

[120] Graeme Edward Minchin, "The Incredible Shrinking Fourth Amendment – The Ongoing Erosion of the Fourth Amendment of the Constitution of the United States of America," Beijing Law Review, September 2021, https://www.scirp.org/journal/paperinformation.aspx?paperid=111625; Gerald G. Ashdown, "The Fourth Amendment and the 'Legitimate Expectation of Privacy,'" 34 Vanderbilt Law Review 1289 (1981).

[121] Beggin, "Questions Arise."

Prohibition that it was unreasonable to require law enforcement to take the time to obtain a warrant while evidence (at the time, alcohol) in a vehicle is readily mobile and could be transported to a secret location.[122] Therefore, police can go into the depths of a car, even take apart the engine, if they so choose, so long as they have probable cause to believe doing so would uncover evidence of a crime.[123] Under this line of precedent, police argue they can extract data directly from a vehicle without a warrant,[124] and some courts decline to give car data full Fourth Amendment protections.[125]

Another troubling Fourth Amendment exception, the third-party doctrine, states that law enforcement can collect information that a person shares with a third party, including a company, without a warrant.[126] The Supreme Court held that individuals do not have a reasonable expectation of privacy in such information, so law enforcement needs neither a warrant nor probable cause to access it.[127] As a result, Fourth Amendment protections arguably disappear when a car beams data to its manufacturer, telematics provider, or insurer.[128]

…And the Good News

Police search powers still have some limitations, such as needing a wiretap warrant prior to recording real-time audio in a car. Courts have held that the Fourth Amendment applies to real-time government wiretaps.[129] Cartapping is analogous to a traditional telephone wiretap and should receive the same protection.[130] Remote access to a person's real-time telematic or infotainment data could be similarly protected. The Supreme Court found that the police may not trespass into a vehicle under the owner's control to install a GPS tracking device without a warrant,[131] though it remains an open question whether such remote access would be permissible without such trespass.

---

[122] Beggin, "Questions Arise."

[123] "Automobile Exception Law," U.S. Legal, Inc.

[124] Gershowitz, "Tesla Meets the Fourth."

[125] *People v. Diaz*, 213 Cal.App.4th 743 (Cal. Ct. App. 2013) *People v. Xinos*, 121 Cal. Rptr. 3d (Cal. Ct. App. 2011); *People v. Christmann*, 3 Misc. 3d 309 (N.Y. Misc. 2004).

[126] Villasenor, "What You Need to Know. *United States v. Miller*, 425 U.S. 435 (1976). S*mith v. Maryland*, 442 U.S. 735 (1979).

[127] Villasenor, "What You Need to Know." *See also, United States v. Miller*, 425 U.S. 435 (1976) (regarding bank records) and *Smith v. Maryland*, 442 U.S. 735 (1979) (regarding pen registers).

[128] Villasenor, "What You Need to Know."

[129] *Katz v. United States,* 389 U.S. 347 (1967).

[130] Cartapping clearly falls within the Wiretap Act. 18 U.S.C. § 2518.

[131] *United States v. Jones*, 615 F. 3d 544 (2012).

Recent Supreme Court precedent has extended Fourth Amendment protections of digital data, though these cases have yet to be applied to car data. In *Riley v. California*, The Supreme Court ruled that searching a cell phone's digital contents during an arrest is unconstitutional unless the police obtain a warrant before doing so.[132] The court reasoned that cellphones store extremely personal data, and that allowing law enforcement unfettered access to that data, even during an arrest, would be too invasive.[133] Infotainment systems download this same personal information when a driver or passenger syncs their device with the vehicle.[134] The fact that courts have yet to hold that downloading cell phone data from a car's infotainment system requires a warrant is an intolerable double standard that the courts must address.

Similarly, in *Carpenter v. U.S*,[135] The Supreme Court held that people maintain a reasonable expectation of privacy in cell tower location information spanning seven or more days, thereby requiring police to obtain a warrant before accessing that data from cell phone service providers in many cases.[136] While written to have a narrow application, the reasoning behind the decision applies broadly to an expectation of privacy in location data, including automobile location information.[137] As a result, the fact that courts have not yet found a reasonable expectation of privacy regarding location data shared between cars and their manufacturers creates a logical inconsistency with Supreme Court case law that courts must immediately remedy.

At least one federal appeals court has also extended constitutional protections to email. The Sixth Circuit found that the Fourth Amendment requires the government to obtain a warrant before compelling emails because "individuals maintain a reasonable expectation of privacy in emails that are stored with, or sent or received through, a commercial Internet Service Provider." [138] This has led to a broader "understanding that the Fourth Amendment ordinarily requires a warrant for government access to email."[139] Courts may apply this reasoning to other forms of information in the future, including messages and other data stored on or transmitted off cars.

---

[132] *Riley v. California*, 573 U.S. 373 (2014).

[133] *Riley*, 573 U.S. 373.

[134] Kinder, "Infotainment Systems."

[135] *Carpenter v. United States*, 585 U.S. ___ (2018).

[136] *Carpenter*, 585 U.S. ___.

[137] *Carpenter,* 585 U.S. ___.

[138] *United States v. Warshak*, 631 F. 3d 266 (6th Cir. 2010). Orin Kerr, "Fourth Circuit Deepens the Split on Accessing Opened E-Mails," *Reason*, March 21, 2019.

[139] Kerr, "Fourth Circuit Deepens Split."

A few state courts are also increasingly affording protection to automobile data. In 2017, a Florida appeals court ruled that event data recorders are analogous to other electronic devices protected by the Fourth Amendment.[140] Subsequently, the highest court in Georgia found that police must obtain a warrant before physically entering a vehicle to remove its stored data.[141] While the constitutional law is still unsettled in other states, these cases show a growing trend of protecting some car data.

B. Additional Protections for Electronic Communications

The federal Electronic Communications Privacy Act (ECPA) grants a limited degree of protection to information held by third parties,[142] but police may argue ECPA does not apply to carmakers. In *JetBlue*, a court reasoned that airlines that maintain websites are not "electronic communications service providers" and fall outside ECPA's scope.[143] This same reasoning may be extended to car companies that offer connected services but outsource the data transfer function. In other words, a court might decide that ECPA only applies to the internet service provider, app developer, or wireless network that transmits data instead of the vehicle manufacturer. That does not mean ECPA never protects car data, but it does mean that the analysis is fact specific.

Even if ECPA does apply in most cases, its strongest protections may not apply to the bulk of car data. ECPA's precise application is fact specific, but in general, police do not need a warrant to access any data a company has stored for over 180 days, at the longest.[144] There has been progress in this area beyond ECPA, as *Warshak* (discussed above) effectively ended the practice of compelling access to the content of communications without a warrant.[145] Still, textually, the strongest protections in ECPA only temporarily delay government access to much vehicle data.[146]

---

[140] *State v. Worsham*, No. 4D15–2733, 227 So. 3d. 602 (Fla. Dist. Ct. App. 2017), https://caselaw.findlaw.com/fl-district-court-of-appeal/1854972.html.

[141] *Mobley v. Georgia,* No. S18G1546 (G.A. 2019), https://law.justia.com/cases/georgia/supreme-court/2019/s18g1546.html.

[142] Electronic Communications Privacy Act, Pub. Law no. 99-508 (1986), https://www.congress.gov/bill/99th-congress/house-bill/4952/text.

[143] *In re JetBlue Privacy Litigation*, 375 F.Supp.2d (E.D.N.Y. 2005).

[144] Electronic Communications Privacy Act (ECPA)," Electronic Privacy Information Center (EPIC), accessed August 15, 2022, https://epic.org/ecpa/.

[145] Jerome Greco comments to the Surveillance Technology Oversight Project, October 11, 2022. Kerr, "Fourth Circuit Deepens Split."

[146] "Electronic Communications Privacy Act," EPIC. Kerr, "Fourth Circuit Deepens Split."

Many states have enacted their own statutes and constitutional protections to supplement ECPA.[147] Thirteen states have adopted constitutional rights to privacy, and most states have laws regulating electronic surveillance to some extent, although they do not necessarily go beyond the protections provided by ECPA.[148] These laws have varying degrees of success in protecting car data. Notably, California's Electronic Communications Privacy Act is broad enough to apply to communications and related data stored on automobiles and requires law enforcement to obtain a warrant before collecting that data in most cases.[149] Likewise, Michigan's constitution requires a warrant before any government search of "electronic data."[150] By its text, this provision appears to include data stored on or collected by vehicles.[151] Unfortunately, in some states, like Missouri, that have enacted additional constitutional protections for electronic data, courts have not extended them to cars when given a chance.[152] And while Florida has been a leader in protecting car data in some ways, it has done worse in others. One Florida court rejected a driver's claim that a local police department violated state law when it used GPS data collected from a tracking device that a third-party owner installed on a loaner car.[153]

The Drivers Privacy Act and related state laws

Congress and state legislatures have taken action to address some vehicle computer systems. In 2015, Congress passed the Driver Privacy Act (DPA),[154] which restricts access to black box information.[155] Under the DPA, law enforcement needs a court order or administrative agency's authorization to access a person's black box without their consent.[156] This affords some protections to black boxes but does not always require a warrant to access their data, and leaves other, more

---

147 See e.g., SB 178, 2015 Regular Sess. (Cal. 2015-2016). HB 126, General Sess. (Utah 2014). HB 2269, 83rd Legislature, Regular Sess (Tex. 2013), "Privacy Protections in State Constitutions," accessed May 4, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

148 A few examples follow. SB 178, 2015 Regular Sess. (Cal. 2015-2016). HB 126, General Sess. (Utah 2014). HB 2269, 83rd Legislature, Regular Sess (Tex. 2013), "Privacy Protections in State Constitutions," accessed May 4, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.Matthisen, Wickert, & Leher, S.C., Laws on Recording Conversations in all 50 States. https://www.mwl-law.com/wp-content/uploads/2018/02/RECORDING-CONVERSATIONS-CHART.pdf

149 R. Taj Moore, "So What's in the California Electronic Communications Privacy Act?," Lawfare, October 22, 2015, https://www.lawfareblog.com/so-whats-california-electronic-communications-privacy-act.

150 Mich. Const. Art 1 Sec. 11.

151 Mich. Const. Art 1 Sec. 11.

152 Mo. Const. Art. I § 15; *State v. West*, 548 S.W.3d 406 (Mo. Ct. App. 2018).

153 *Bailey v. State*, No. 1D18-4514 (Fla. Dist. Ct. App. 2020).

154 S. 766, 1st Sess. 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/766/text.

155 S. 766, 1st Sess. 114th Cong. (2015).

156 S 766, 1st Sess. 114th Cong. (2015).

personally revealing areas of the car—the telematics and infotainment systems—entirely open.[157] Seventeen states have enacted legislation similar to the DPA.[158] Of the seventeen, only New Jersey and Montana include a full warrant requirement for law enforcement access to black boxes.[159]

The Safeguards Rule and related state laws

The Safeguards Rule issued under the Gramm-Leach-Bliley Act (GLBA) provides protection for car data held by financial institutions, such as companies that lease or finance cars, including dealerships. The Safeguards Rule requires financial institutions to develop procedures for the disposal of customer information no more than two years after the last interaction with a customer unless the company has a valid business reason to retain the data.[160] If properly enforced, the Safeguards Rule could spur car financers to delete sensitive data that doesn't serve an identified and defensible business purpose—making less information available to law enforcement by ensuring the data no longer exists.[161]

Similarly, thirty three states have implemented versions of a model bill regulating data stored by insurance companies that could lead to insurance companies storing less car data.[162] The National Association of Insurance Commissioners' Model Bill 673 requires insurance companies to "implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information."[163] Insured drivers' information is stored on insurers' own servers if they offer insurance discounts for telematics. In many cases, deleting this data within a reasonable time is the simplest way to comply with the Model Bill's safeguards requirement. If properly enforced, state insurance laws could rally insurers to reduce their data and limit its availability to police.

---

[157] S 766, 1st Sess. 114th Cong. (2015).

[158] "Privacy of Data from Event Data Recorders: State Statutes," National Conference of State Legislatures, January 25, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

[159] "Privacy of Data," National Conference.

[160] 86 FR 70272 (5)I(6)(i).

[161] 86 FR 70272 (5)(c)(6)(i).

[162] Tom Ham, "Laws by Geography," Privacy4Cars, accessed August 31, 2022, https://privacy4cars.com/legal-resources/laws-by-geography/.

[163] Model Bill 673, National Association of Insurance Commissioners, accessed August 31, 2022, https://content.naic.org/model-laws.

VI. RECOMMENDATIONS

A. Recommendations for lawmakers

1. Pass legislation to limit the collection, retention, and sharing of data

The collection and retention of automobile data is dangerous, even if law enforcement agencies are limited in their ability to harvest it. Not only can retained data be sold (and purchased by law enforcement—a common tactic to avoid Fourth Amendment obligations),[164] it is also vulnerable to hackers.[165]

The U.S. and states must expand on the Safeguards Rule, DPA, and other privacy statutes to ban the collection of, ban the sale of, and implement strict retention schedules for location history, communications data, and biometric information.[166] The schedules should be proportional to the data points' sensitivity and value.[167] This would mean, at minimum, deleting nonessential communications, biometrics, and location data after every trip and giving consumers a right to delete their data from vehicles and servers.

Similarly, new laws should give motorists greater control by requiring vehicle manufacturers to obtain data subjects' opt-in consent before collecting or distributing their information.[168] Importantly, the legislation must specify that there should be no penalty against individuals who opt out of data collection, retention, or distribution. It should also include prohibitions on bundling discrete forms of data collection under a single consent request. For instance, combining permissions to dial an emergency call system with permissions for persistent location tracking results in a broader scope of consent than is necessary to operate the calling system. Lawmakers should also recognize a driver's right to have all non-essential data stored locally and their right to encrypt their car to prevent the unauthorized sharing and retrieval of their personal information.

---

[164] Laura Hecht-Felella, "Federal Agencies Are Secretly Buying Consumer Data," Brennan Center, April 16, 2021, https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.

[165] Laura Hoffner, "Hacking Is the New Car Jacking: How To Secure Vehicle Data," *CPO Magazine*, January 14, 2022, https://www.cpomagazine.com/cyber-security/hacking-is-the-new-car-jacking-how-to-secure-vehicle-data/.

[166] This recommendation is like the common practice of designating some information as being especially sensitive and thus necessitating stronger protections. California adopts this approach under the Consumer Privacy Rights Act (CPRA). "Annotated Text of the CPRA with CCPA Changes," Yes on Prop 24, accessed May 6, 2022, https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/.

[167] This approach is the same in principle to the CPRA's and General Data Protection Regulation's (GDPR) retention schedule mandates. See "Robust Data Retention Programs Required By New Laws," Squire, Patton, Boggs LLP, May 18, 2021, https://www.consumerprivacyworld.com/2021/05/robust-data-retention-programs-required-by-new-laws/.

[168] This is similar to the GDPR's opt-in requirement. Rita Heims, "How Opt-in Consent Really Works," International Association of Privacy Professionals, February 22, 2019, https://iapp.org/news/a/yes-how-opt-in-consent-really-works/.

Legislators must enact laws requiring police to obtain a warrant before accessing car data, whether from the car itself or from a company storing the data. The warrant must be supported by probable cause and individualized suspicion of criminal wrongdoing, be narrowly tailed, and be subject to independent oversight. States should also consider passing legislation that builds a legal firewall between transportation agencies and the police, preventing agencies from sharing personal information with law enforcement without a warrant. This creates the minimum necessary protections by bringing automobile data in line with the protections of the U.S. Constitution and creates a baseline from which lawmakers can make further improvements.

Legislatures also must prohibit law enforcement from using tools that capitalize on the sensitivity of biometric identifiers and location data, including facial recognition technology and geofence warrants. Vehicle-derived biometric data could give agencies a years-long record of every time a person blinked or glanced away from the road while driving, or even rode in the car as a passenger. This level of surveillance introduces new and serious risks to driving, including the misidentification of BIPOC drivers, the wrongful ascription of inattentiveness to drivers who experience involuntary affects and tics, and the extension of police surveillance into car interiors.

2. Administrative rulemaking and enforcement

Administrative agencies like the Federal Trade Commission (FTC) should engage in rulemaking and enforcement actions related to car data. The FTC should use its Unfair and Deceptive Acts and Practices (UDAP) authority to levy penalties against companies that misrepresent the extent of their own privacy practices, such seeking judgments against companies that deceptively claim to comply with industry recognized privacy principles.[169] Similarly, the FTC should consider using its UDAP powers to promulgate regulations to prevent harmful surveillance practices before they occur.[170] These regulations should, at least, track the recommendations put forward in in the section above.

The Federal Communications Commission (FCC) should also consider taking up regulatory and enforcement activities targeted towards telematics companies and their network partners. To provide services, telematics companies purchase wireless network bandwidth to share data and

---

[169] Matt Hudson, "Vehicle Data: A Look at OEM Principles," Adapt Automotive, February 21, 2020, https://www.adaptautomotive.com/articles/110-vehicle-data-a-look-at-oem-principles.

[170] Lesley Fair, "FTC Undertakes Inquiry into Commercial Surveillance Practices and Wants Your Insights," Federal Trade Commission, August 16, 2022, https://www.ftc.gov/business-guidance/blog/2022/08/ftc-undertakes-inquiry-commercial-surveillance-practices-wants-your-insights.

communications,[171] and therefore, much of the telematics sector is made up by mobile virtual network operators and other telecom companies under FCC jurisdiction.[172] Telecom companies already must comply with stronger privacy rules than many other corporations.[173] The FCC could improve privacy protections for motorists by using this authority to regulate and bring enforcement actions against telematics providers and related companies.

B. Recommendations for companies

Vehicle manufacturers and other companies must amend their data policies and user interfaces to recognize the sensitivity of car data.[174] Automakers must recognize that lawful police use of car data poses a threat to drivers and passengers. Companies should voluntarily implement opt-in requirements before collecting communications, location history, and other sensitive data to be stored on the vehicle or on remote servers. Additionally, companies should not use data for any purpose out of step with reasonable consumer desires. They should also make it easier for motorists to delete data permanently. If motorists do not delete the data on their own, companies should automatically delete it when it is not necessary to retain the information.

Specifically, companies should not store data in a way where it can be used for geofence and other dragnet searches by law enforcement. As outlined in Section IV, car-based location data could easily reveal vehicles present at particular locations at specified times, where those cars started and ended the day, and vehicles that drove along particular routes. If companies refuse to store this data, they will not have anything to turn over when prosecutors demand this type of data via subpoena or search warrant, or when law enforcement tries to buy it. Companies should not store multiple, non-

---

171 "KORE to Provide Connectivity for Intelligent Telematics Partnership," KORE Group Holdings, Inc., accessed September 27, 2022, https://ir.korewireless.com/news-events/press-releases/detail/64/kore-to-provide-connectivity-for-intelligent-telematics. "Pareteum for the Automobile Industry," Pareteum, accessed September 27, 2022, https://www.pareteum.com/connected-cars-internet-of-vehicles-iov/. "Globalmatix and Thales Put Vehicle Telematics in the Fast Lane," Thales Group, accessed September 27, 2022, https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/customer-cases/globalmatix. "Embracing MVNOs and Connected Cars with Policy," *Cisco Blogs* (blog), April 16, 2015, https://blogs.cisco.com/sp/embracing-mvnos-and-connected-cars-with-policy.

172 Declaration of Thomas W. Hazlett before the Federal Communication Commission In the Matter of Fostering Innovation and Investment in the Wireless Communications Market A National Broadband Plan For Our Future, https://www.att.com/Common/about_us/public_policy/fcc_wireless_noi/Declaration-Hazlett.pdf. Federal Communications Commission, Notice of Apparent Liability for Forfeiture, August 5, 2022, https://docs.fcc.gov/public/attachments/DA-22-825A1.pdf.

173 Danielle Letenyei, "What Is CPNI and Should Cellphone Users Opt Out to Protect Themselves?," Market Realist, November 3, 2021, https://marketrealist.com/p/should-i-opt-out-cpni/. There are restrictions on telecom companies use of customer identifying information. "Customer Privacy," Federal Communications Commission, March 3, 2011, https://www.fcc.gov/general/customer-privacy. Kelly Hill, "FCC to Investigate Carriers' Use of Subscriber Location Data," *RCR Wireless News*, August 30, 2022, https://www.rcrwireless.com/20220830/policy/fcc-to-investigate-carriers-use-of-subscriber-location-data.

174 This is an example of "privacy by design." "Privacy by Design," Intersoft Consulting, accessed May 6, 2022, https://gdpr-info.eu/issues/privacy-by-design/.

aggregated location records in a relational database. Data should be completely anonymized so that it cannot reasonably be used to infer information about, or otherwise be linked to a particular consumer, household, or device.

Likewise, manufacturers should consider whether they truly need to collect and for how long to store sensitive information.[175] If they decide that such data is not necessary, or that countervailing risks to motorists outweigh the data's value, they should build processes that prevent its storing and sharing. It is important that companies center their customers' interests rather than their corporate interests, including the profits that could be made from selling customers' private data.

VII. CONCLUSION

It is time to put the brakes on law enforcement's access to car data. Some of this data is arguably pedestrian, reflecting vehicle performance and accident information, but other data is deeply private, including location history, communications, and biometric identifiers. This sensitive information deserves strong protection to keep motorists safe on the road from subversion of their constitutional rights and wrongful prosecution.

[175] This is an example of a legitimate interest test. "What Is the 'Legitimate Interests' Basis?," Office of the Information Commissioner for the United Kingdom, January 1, 2021, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT