Vehicular Surveillance

RESTORE the FOURTH

What are Connected and Autonomous Vehicles (CAVs)?

Connected and autonomous vehicles (CAVs) constitute a radical change to our everyday travel. CAVs combine a series of technologies – GPS navigation, advanced vehicle-sensors, telematics, wireless communication, and automated computing – to remove the possibility of human error while driving and to improve road safety. CAVs operate within a broader network of highway and road communication technologies, a process referred to as vehicle to infrastructure communication (V2I). Highway communication and monitoring technology encompasses a plethora of devices: automated license plate readers (ALPR), Bluetooth detection systems, Flock safety cameras, electronic tolling, and other technologies.[1]

Whether they are safe overall, or safer relative to the average human driver, is beyond Restore the Fourth's remit. But we know privacy, and this brief assesses the privacy and Fourth Amendment implications of broader adoption of CAVs.

In a recent Hearing on Equity in Transportation Safety Enforcement of the U.S. House Highways and Transit Subcommittee, representatives stated that far too often individuals are stopped for reasons other than traffic safety violations, and that ensuring safety on our roadways means not only protecting people from dangerous drivers but protecting people from enforcement abuses.[2]

CAVs and roadway monitoring systems have proliferated as a result of their promise to improve a variety of problems on the road, including traffic, speeding, accidents, pollution and toll collection. But these purported benefits obscure the value of such systems to police, in creating a real-time flood of data on vehicles' movements. By doing so, these systems pose a grave risk to the Fourth Amendment, which should require police to get a warrant to obtain the pattern of people's movements through public space. It's no wonder that these systems are unpopular: A study conducted by the American Automobile Association (AAA) found that 72% of Americans expressed fear or hesitancy toward CAV use.[3]

CAVs collect massive troves of data to function: driver biometric and health data from a steering wheel heart rate monitor or health devices synced through Bluetooth (such as fitness monitors); driver's visual attention to the road as recorded by a dashboard sensor; data services accessed (phone use, contacts, emails, website browsing and application use histories, radio station consumption); and vehicle location, speed, and occupancy. Current law also requires in all new vehicles by 2024, technological tracking of drivers' sobriety and attentiveness.[4]

DHS has poured millions into the Heedful Audio Alert System (HAAS), a cellular V2V app that alerts drivers to the presence of law enforcement and first responders. Sometimes called R2V, or a Responder to Vehicle Program, HAAS allows direct communication between law enforcement and vehicles.[5]

CAVs and roadway surveillance technology constitute a mass surveillance network that has the dystopian potential to track our daily lives, data point by data point. One car trip may not paint a detailed picture of one's life, but the repeated tracking of a vehicle creates a mosaic of information that law enforcement can weaponize. If the data is already pro-actively collected, then it presents too much of a temptation to law enforcement to dip into it not only when someone is suspected of a violent crime, but also to track protesters, people seeking abortion care, and people fleeing government persecution. In short, they threaten our Fourth Amendment and First Amendment rights, in ways that venture capitalists may not really care much about.

The remainder of this brief presents privacy concerns specific to CAVs and their manufacturers, outlines the current legal standing of vehicle surveillance technology, and concludes with a series of policy and action recommendations created by our activists here at Restore the Fourth.

CAV Privacy Concerns

Vehicles are no longer just mechanical devices. CAVs possess hundreds to thousands of Electronic Control Units (ECU) that run code constantly to operate their communications and sensor technologies.[6] Vehicles are exposed to all of the problems and dangers associated with stored data and communications technology, including being hacked. A study conducted in 2010 tested to see if remote attack of CAVs was possible.[7] They found that remote exploitation of CAVs is not only possible, but highly likely given the broad range of attack surfaces available to a potential hacker. These surfaces include but are not limited to: Bluetooth, keyless remote entry, telematics connected to the internet, and VANET, as well as the abundance of vehicle sensors (cameras, lidar, radar, GPS, tire pressure measure sensors (TPMS), inertial measurement units (IMUS), and engine control sensors.[8] Hackers – or governments – could use these to seize your car's data or, worse, your car's controls.

Policy that ensures CAV data protection is almost nonexistent. As the Texas A&M Institute explains, in the United States, "There is no single comprehensive legislative framework for data privacy protection. There is also no single regulatory authority. Most states have enacted some form of privacy legislation. However, there is no regulatory framework that specifically addresses connected car data."[9] The only regulatory efforts in CAV data protection currently are a set of industry guidelines and standards that are not legally binding. The loose and noncommittal nature of these guidelines means that automotive companies do not completely follow standards that protect user privacy.[10]

According to a GAO report that found widespread privacy policy noncompliance, *all* of the ten largest companies that offer or use in-car location-based services had privacy policies that were lacking, unclear or illegible.[11] Most disclosure agreements were too broad and unclear. Consent for data collection was there, but consumers could not opt out of data retention. All ten use different de-identification methods, with varying effectiveness. Nine share the vehicle data they collect with various third parties, but not including data brokers or marketers. As for the 13 largest companies that produce CAVs or offer CAV services, none of them were shown to substantially demonstrate leading industry practices for privacy protection (transparency, focused data use, data security, data access and accuracy, individual control, and accountability).[12]

Automated License Plate Readers (ALPRs)

ALPRs illustrate the broad scope of data collection on our roads. ALPRs are small cameras that are mounted on road signs, stationary infrastructure, or on the back of police cars. These devices record images of passing vehicles non-stop to identify and track license plate information. Collected images are stored in a database along with GPS information and timestamps. Tens of thousands of ALPRs exist in the U.S. In 2016 and 2017 alone, 2.5 billion license plates were scanned by 173 law enforcement agencies as well as private actors.[13]

ALPRs are regularly used in biased and discriminatory ways. NYPD used ALPRs to spy on those attending services at mosques across the country.[14] ALPRs are deployed to monitor political protesters and activists, in blatant disregard for First and Fourth Amendment rights.[15] Some police departments incorporate ALPR technology into Real Time Crime Centers (RTCCs),[16] enabling ICE, CBP, and DHS to use them to pursue undocumented immigrants, sometimes contravening local 'sanctuary city' laws.[17] In Los Angeles, ALPRs are part of Operation LASER, which warrantlessly collected data on anyone police encountered to make solving crimes easier in the future.[18] Operation LASER prioritized quantity over accuracy, intensifying policing in already overpoliced communities.

Pictures taken by ALPRs often include more than just a license plate – vehicle occupants, the surrounding area, and other vehicles nearby can be caught. This data is retained indefinitely and widely shared with private companies, other government agencies, and fusion centers.[19] Private companies, like Rekor Systems Inc., develop sprawling networks of ALPR readers. They provide continual, real-time access to the data their network collects and refines at little to no cost – that's over 150 million

plate reads per month.[20] Rekor's CEO claims, "This network exists to help law enforcement prevent and solve crimes through a shared resource."[21] However, 99.5% of license plates scanned are not under suspicion of criminal activity, so data on a very large number of innocent motorists' movements is being gathered for a very small return.[22]

Auto-Hacking and Security Vulnerabilities

There has been one corroborated instance of a purposeful and malicious remote attack on vehicles. In 2010, a former Texas Auto-Center employee remotely disabled 100 vehicles via internet-connected systems linked to a delinquent car payment program.[23] Other reports detail thieves disabling lock-systems in parked vehicles however they required close proximity to the vehicle.[24]

The vulnerability of CAVs to cyberattacks appears to be a theoretical situation with potentially disastrous consequences. Researchers have conducted numerous experiments that demonstrate modern vehicles with computing or internet capabilities are vulnerable to remote attack and surveillance. For example, a research team was able to send commands through a vehicle's infotainment system to control dashboard functions, steering, brakes, and transmission all from a remote laptop.[25] They found up to 47,000 vehicles vulnerable to their remote control. Similarly, another researcher was able to gain access to 25 Tesla vehicles across the world.[26]

In 2011, research teams from the University of Washington and University of California at San Diego demonstrated that they could wirelessly disable brakes and locks on a sedan through a myriad of attack surfaces.[27] In one study, it was shown that with possession of a Vehicle Identification Number (VIN) one could pull reams of personal information stored in a vehicle from telematics systems operated by SiriusXM.[28] Over 10,000 different car models were vulnerable to this exploit, leaving highly personal information like email addresses, phone numbers, home addresses, IP addresses, phone activity, and regularly frequented public and private locations at risk.

CAV security vulnerabilities led Senators Edward J. Markey (D-Massachusetts) and Richard Blumenthal (D-Connecticut) to introduce the Security and Privacy in Your Car Act of 2015, or the "SPY Car Act."[29] The bill purported to establish cybersecurity requirements for automotive manufacturers and to imbue the Federal Trade Commission (FTC) with the power to enforce stricter data privacy and use regulations.[30] Although this bill did not pass, there are other legal frameworks concerned with CAV cybersecurity. The United Nations Economic Commission for Europe (UNECE) established cybersecurity performance and audit requirements as of 2020, which currently apply to 54 countries, including the U.S.[31]

While these legal protections are important, protecting CAV users from the theoretical dangers of remote hackers seems misguided given previous government efforts to obtain private data from vehicles through similar means. Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), both agencies under DHS purview, purchase "vehicle forensics" technology sold by Swedish data extraction firm MSAB and manufactured by Berla, a U.S. company.[32] ICE and CBP have spent close to one million dollars in a single month on vehicle spying tools.[33] For border enforcement agencies like ICE and CBP, the granular location data collected by modern vehicles provides a quick, cost-effective, and more direct method to track and apprehend a suspect than a warranted search. These extraction tools circumvent the Fourth Amendment's protection against unreasonable searches. ICE and CBP also rely on the fact that their data extraction operations happen without the user knowing, like a remote hacker looking to obtain private information. Intelligence agency capability in this area may by now be widespread, if hard to prove; in 2013, former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism Richard A. Clarke, acknowledged that, "There is reason to believe that intelligence agencies for major powers—including the United States—know how to remotely seize control of a car."[34]

While the threat of remote hackers remains largely hypothetical, the specter of data-hungry government agencies spying on motor vehicle operators is a present and dangerous reality.

Vehicular Surveillance and Fourth Amendment Law

CAVs present new challenges to existing Fourth Amendment protections for motorists and raise complicated legal questions:

- How does the large amount of personal data collected by CAVs affect the 'automobile exception' to the Fourth Amendment?
- How applicable are Court rulings governing cellphone privacy protections to cars, when we consider that CAVs often connect to smartphones and store their data?
- Should law enforcement officers need a warrant to search a CAV, or can previous vehicular exceptions to the warrant requirement be applied to this new technology?
- How does the Fourth Amendment protect the privacy interests implicated by CAVs?

The Court has not decided on a case involving a CAV. The legal history of the Fourth Amendment has treated automobiles distinctly from other protected properties like houses.[35] A series of Court rulings, dating back to Carroll v. United States (1925), established that a law enforcement officer only needs a reasonable, individualized suspicion to stop vehicles, and probable cause can be established during the stop to justify a search in lieu of a warrant.[36] This precedent, referred to as the "automobile exception," has paved the way for warrantless surveillance of vehicles and motorists.

Despite the weaker Fourth Amendment protections afforded to motorists, the sheer amount of personal and private data CAVs collect necessitates a reconsideration of precedent.[37] Indeed, that process has already begun. Three recent Supreme Court rulings demonstrate that CAVs should be afforded stronger Fourth Amendment protections: Riley v. California, U. S. v. Jones, and Carpenter v. United States. Riley v California established that cell phones are not subject to the search incident to arrest exception or closed container designation; an officer needs a warrant to conduct a search of a cell phone's contents, even if it is seized in a vehicle pursuant to arrest.[38] Since CAVs both store cellphone data and collect similar data, Riley v. California should govern the Court's decision in any future case involving CAVs.

United States v. Jones (2012) dealt with the question of whether a tracking device physically attached to a vehicle by a law enforcement officer to monitor its movements on public streets constitutes a Fourth Amendment violation.[39] The Court held that Jones's Fourth Amendment rights were violated. The Court based their ruling on the fact that the officer violated the physical integrity of the vehicle and did not base their decision on the privacy interests involved in GPS data. Nonetheless, the Court recognized that the "substantial quantum of intimate information" that vehicular GPS data provides alters "the relationship between citizen and government." Jones implicitly recognizes that GPS data will need to be protected from discretionary automobile policing, whether that tracking is physical or remote.

The Court has consistently held that there is not a legitimate claim to privacy in information shared with third-parties, a principle referred to as the "third-party doctrine" of the Fourth Amendment.[40] However, the ubiquity of smartphones has brought this legal principle into question. In Carpenter v. United States (2018), the Court denied the state's access to a wireless carrier's cell-site location information (CSLI).[41] The majority reasoned that information from unavoidable and expansive CSLI data collection deserves Fourth Amendment protections despite it being shared with a third-party. The same reasoning would apply to CAV data collection, which shares the same depth of collection as cellphones. Just as smartphone technology did, the widespread use of CAV technology is firm grounds to argue for the obsolescence of the third-party doctrine.

What Does Restore the Fourth Recommend?

To protect motorists' Fourth Amendment rights, Restore the Fourth recommends the following actions:

1. Automakers must give consumers the option to disable all data collection and sharing without denying them access to core automotive features like cruise control.
2. Automakers must make every effort to collect only the data necessary for consumer and vehicle safety, repair, and popular consumer services. Regulators should establish what constitutes "necessary data."
3. Automakers must provide to all consumers a complete description of their privacy policy, written clearly in plain English and other languages as appropriate, in the U.S. market.
4. Owners of a vehicle must be informed that it is their responsibility to ensure that additional drivers are aware of the privacy policy.
5. Consumers should be given the opportunity opt out of sharing some types of data without losing access to all services. While some minimum data sharing is necessary for receiving "core" connected services—such as roadside assistance and crash response—consumers should be able to opt out of sharing other data and forego other services such as Wi-Fi and hands-free calling.
6. Automakers must make every effort to protect consumer data by limiting data access to certain company staff, using firewalls and encryption, and using penetration testing and code reviews.
7. Automakers must conduct privacy risk assessments, which would involve determining the sensitivity of the collected data and the potential risks if the data were improperly lost, accessed, or disclosed. These risk assessments should also evaluate third parties' use of data collected from connected vehicles.
8. Automakers should not be able to share connected vehicle data unless they have the consumer's explicit consent or have been issued a warrant for specific data.
9. Consumers must have the opportunity to review their data for accuracy.
10. Consumer consent should be required for dealerships, independent mechanics, or automobile insur¬ance companies to access vehicle data, and there should be limits on how long data can be retained.
11. Only de-identified data should be accessible for use in research, traffic control, or marketing.
12. Data shared for the purpose of roadside assistance should be clearly defined by regulators, as should a limit on how long such data may be kept by the service provider.
13. Privacy practices must be communicated to all employees as well as to any third parties (e.g., telecommunications companies, telematics service providers, and content providers), and the latter must agree to the privacy practices in their contractual agreements.
14. Automakers must keep clear records of when, to whom, for how long and exactly what purpose private data is shared.
15. Regulators must conduct regular audits of company privacy practices.
16. Automakers must be held legally responsible for data protection.

Endnotes

1 Joseph Cox, "Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras," Vice, March 3, 2021, https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader.

2 "EXAMINING EQUITY IN TRANSPORTATION SAFETY ENFORCEMENT," Legislation, Congress.gov, February 24, 2021, http://www.congress.gov/.

3 "Fact Sheet: Consumer Sentiment on Automated Vehicles" (American Automobile Association, 2020), NewsRoom.AAA.com.

4 Ian Duncan, "New Technology Mandate in Infrastructure Bill Could Significantly Cut Drunken Driving Deaths," Washington Post, November 9, 2021, https://www.washingtonpost.com/transportation/2021/11/09/drunk-driving-technology-infrastructure/.

5 Joe Cadillic, "DHS Wants to Let Police and Emergency Vehicles Talk to Your Car," MassPrivateI: Privacy, Civil Rights, and Homeland Insecurity (blog), 2018, https://massprivatei.blogspot.com/2018/10/dhs-wants-to-let-police-and-emergency.html.

6 Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in 20th USENIX Security Symposium (USENIX Security 11) (San Francisco, CA: USENIX Association, 2011), https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces.

7 Checkoway et al.

8 Zhendong Wang et al., "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey," Sustainability 14, no. 19 (January 2022): 12409, https://doi.org/10.3390/su141912409.

9 Johanna Zmud, Melissa Tooley, and Matthew Miller, "Data Ownership Issues in a Connected Car Environment: Implications for State and Local Agencies," Technical (Texas A&M Transportation Institute, 2016).

10 "Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers" (United States Government Accountability Office (GAO), 2013).

11 "Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers."

12 "Vehicle Data Privacy: Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role" (United States Government Accountability Office (GAO), 2017).

13 Tanvi Misra, "How Worried Should You Be About Automated License Plate Readers?," Bloomberg, December 6, 2018, https://www.bloomberg.com/news/articles/2018-12-06/why-privacy-advocates-fear-license-plate-readers; Dave Maass and Beryl Lipton, "What We Learned," MuckRock, November 15, 2018, https://www.muckrock.com/news/archives/2018/nov/15/alpr-what-we-learned/.

14 Adam Goldman and Matt Apuzzo, "With Cameras, Informants, NYPD Eyed Mosques," Associated Press, February 23, 2012, https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

15 "You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements" (American Civil Liberties Union (ACLU), 2013)

16 Vasudha Talla, "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations," American Civil Liberties Union, March 12, 2019, https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data.

17 Suhauna Hussain and Johana Bhuiyan, "California Police Share License Plate Data with ICE," GovTech, December 21, 2020, https://www.govtech.com/public-safety/California-Police-Share-License-Plate-Data-with-ICE.html; Kate Cox, "CBP Does End Run around Warrants, Simply Buys License Plate-Reader Data," Arstechnica, 2020, https://arstechnica.com/tech-policy/2020/07/cbp-does-end-run-around-warrants-simply-buys-license-plate-reader-data/; "Homeland Security - Real-Time Crime Center - City of New Orleans," Office of Homeland Security and Emergency Preparedness, accessed May 22, 2023, https://nola.gov/homeland-security/real-time-crime-center/.

18 Mara Hvistendahl, "How the LAPD and Palantir Use Data to Justify Racist Policing," The Intercept, January 30, 2021, https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing/.

19 "You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements."

20 Adam Frost, "Rekor Launches Public Safety Network of ALPR Data for Law Enforcement Agen-

cies," Traffic Technology Today (blog), August 27, 2019, https://www.traffictechnologytoday.com/news/machine-vision-alpr/rekor-launches-public-safety-network-of-alpr-data-for-law-enforcement-agencies.html.
21 "Rekor Systems Launches Public Safety Network," Bloomberg.Com, August 21, 2019, https://www.bloomberg.com/press-releases/2019-08-21/rekor-systems-launches-public-safety-network.
22 Dave Maass and Beryl Lipton, "Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers," Electronic Frontier Foundation, November 15, 2018, https://www.eff.org/pages/automated-license-plate-reader-dataset.
23 Kevin Poulsen, "Hacker Disables More Than 100 Cars Remotely," WIRED, March 17, 2010, https://www.wired.com/2010/03/hacker-bricks-cars/.
24 Nick Bilton, "Keeping Your Car Safe From Electronic Thieves - The New York Times," New York Times, 2015, https://web.archive.org/web/20220224230147/https:/www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.
25 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," WIRED, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
26 David Colombo, "How I Got Access to 25+ Tesla's around the World. By Accident. And Curiosity.," https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028.
27 Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces."
28 Thomas Brewster, "Cops Can Extract Data From 10,000 Different Car Models' Infotainment Systems," Forbes, 2022, https://www.forbes.com/sites/thomasbrewster/2022/12/01/10000-cars-can-be-data-raided-by-police-ice-cbp-love-it/?sh=25f1cd69d807.
29 Ed Markey and Richard Blumenthal, "Security and Privacy in Your Car Act of 2015" (2015), https://www.congress.gov/bill/114th-congress/senate-bill/1806/text.
30 Andy Greenberg, "Senate Bill Seeks Standards For Cars' Defenses From Hackers," WIRED, July 21, 2015, https://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/.
31 "WP.29 Cybersecurity Vehicle Regulation Compliance," Blackberry QNX, https://blackberry.qnx.com/en/ultimate-guides/wp-29-vehicle-cybersecurity.
32 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/.
33 Brewster, "Cops Can Extract Data From 10,000 Different Car Models' Infotainment Systems."
34 Mike Hogan, "Was Michael Hastings' Car Hacked? Richard Clarke Says It's Possible," Huffington Post, 2013, sec. Entertainment, https://www.huffpost.com/entry/michael-hastings-car-hacked_n_3492339.
35 Tracey Maclin, "Cops and Cars: How the Automobile Drove Fourth Amendment Law," Boston University Law Review 99, no. 5 (2019).
36 Carroll v. United States, No. 15 (U.S. Supreme Court 1925).
37 Lindsey Barrett, "Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception," Georgetown Law Journal 106, no. 1 (2017).
38 Riley v. California (California Fourth District Court of Appeals 2014).
39 United States v. Jones, No. 10-1259 (U.S. Court of Appeals for the District of Columbia Circuit 2012).
40 Tracy Pearl, "The Fourth Amendment in the Age of Autonomous Vehicles," George Mason Law Review, 2022.
41 Carpenter v. United States, No. 16-402 (U.S. Supreme Court 2018).