epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION/DEPARTMENT OF TRANSPORTATION

Request for Comment on "Federal Automated Vehicles Policy"

Docket No. 2016-22993

November 22, 2016

By notice published on September 23, 2016 the National Highway Traffic Safety Administration ("NHTSA") requests public comments on the Federal Automated Vehicles Policy.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to highlight the privacy and safety risks of automated vehicles and to recommend that NHTSA revise the Automated Vehicle Policy to: (1) require mandatory compliance with the Consumer Privacy Bill of Rights ("CPBR"); (2) include more effective oversight and enforcement mechanisms; and (3) abandon efforts to preempt state law.

[1] *Request for Comment on "Federal Automated Vehicles Policy,"* 81 Fed. Reg. 65,703 (Sep. 23, 2016).

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has worked extensively on the privacy and data security implications of connected cars.[2] EPIC has also submitted numerous comments to NHTSA on privacy issues raised by networked vehicles.[3]

I. AUTOMATED VEHICLES PRESENT SUBSTANTIAL PRIVACY AND SAFETY RISKS

New vehicle technologies offer a variety of beneficial services to American drivers, and are being quickly implemented by car manufacturers. But these new technologies also raise substantial privacy and safety concerns that must be addressed through meaningful, legally enforceable safeguards. Current approaches, based on industry self-regulation, are inadequate and fail to protect driver privacy and safety. NHTSA must issue mandatory rules to address the myriad risks posed to drivers operating vehicles in the United States.

---

[2] EPIC Associate Director Khaliah Barnes, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public Assets, *The Internet of Cars* (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony- Nov-18-2015.pdf; Brief of Amicus Curiae EPIC, *Cahen v. Toyota Motor Corporation*, No. 16-15496 (9th Cir. Aug. 5, 2016), https://epic.org/amicus/cahen/EPIC-Amicus-Cahen-Toyota.pdf; Marc Rotenberg, *Are Vehicle Black Boxes a Good Idea?*, THE COSTO CONNECTION (Apr. 2013), http://www.costcoconnection.com/connection/201304?pg=24#pg24; Marc Rotenberg, *Steer Clear of Cars That Spy*, USA TODAY (Aug. 18, 2011), http://usatoday30.usatoday.com/news/opinion/editorials/2011-08-18-car-insurance-monitors-driving-snapshot_n.htm.

[3] *E.g.*, EPIC, Comments on the Federal Motor Vehicle Safety Standards: "Vehicle-to- Vehicle (V2V) Communications", Nat'l Highway Traffic Safety Admin., Docket No. NHTSA-2014-0022 (Oct. 20, 2014), https://epic.org/privacy/edrs/EPIC-NHTSA- V2V-Cmts.pdf; EPIC et al., Comments on the Federal Motor Vehicle Safety Standards; Event Data Recorders, Nat'l Highway Traffic Safety Admin., Docket No. NHTSA- 2012-0177 (Feb. 11, 2013), https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf; *see generally* EPIC, *State Auto Black Boxes Policy* (2015), https://epic.org/state-policy/edr/; EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy* (2015), https://epic.org/privacy/edrs/.

A. Automated Vehicles Collect and Broadcast Troves of Sensitive Personal Data

Modern cars contain dozens of small computers that are linked together by the car's internal computer network.[4] These computers control everything from braking, acceleration, steering, engine performance, door locks, and climate control to navigation and entertainment.[5] As cars become more technologically sophisticated, they acquire the ability to collect and disclose huge amounts of sensitive driving data. According to a 2015 Senate report, about a third of all of cars from 13 major car manufacturers contain technologies that collect driving history information.[6] These technologies include "navigation, telematics, infotainment, emergency assist, stolen vehicle recovery, and event data recording systems."[7]

Many modern cars contain "telematics" systems, which "use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider."[8] According to 2014 Government Accountability Office ("GAO") testimony, the collection and disclosure of consumer location information by in-car navigation providers pose serious risks to consumer privacy.[9] Storing location information over time

---

[4] *See Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Sen. Edward J. Markey (D-Mass) (Feb. 2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [hereinafter "Markey Report"]; David Gelles, Hiroko Tabuchi & Matthew Dolan, *Complex Car Software Becomes the Weak Spot Under the Hood*, N.Y. TIMES (Sep. 26, 2015), http://www.nytimes.com/2015/09/27/business/complex-car-software- becomes-the-weak-spot-under-the-hood.html?_r=0; 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/.

[5] *See* Gelles, Tabuchi & Dolan, *supra* note 5; Greenberg, *supra* note 5.

[6] *See Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Sen. Edward J. Markey (D-Mass.) (Feb. 2015) at 8, https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [hereinafter "Markey Report"].

[7] *Id*.

[8] U.S. Gov. Accountability Office, GAO-14-649T, *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers* (2014), http://gao.gov/products/GAO-14-649T.

[9] *Id*. at 2.

"create[s] a detailed profile of individual behavior, including habits, preferences, and routes traveled," the exploitation of which can lead to identity theft or threats to personal safety.[10] In particular, the GAO report noted that in-car navigation providers "use different de-identification methods that may lead to varying levels of protection for consumers."[11]

Driverless cars generate even more data, with cameras and sensors collecting information from inside the car and its exterior surroundings.[12] For example, BMW's in-car sensors can detect whether a child is on board.[13] Demand for access to vehicle information is growing. Ian Robertson, the sales and marketing board member for BMW, warned that advertisers have been pressuring carmakers for vehicle information.[14] According to Robertson, advertisers are eager to know, for example, how long a car has been running to determine "from the navigation system, they're about to pass a McDonald's, the car's been running for three hours and the child's probably hungry."[15]

This trend is especially concerning given the role that companies like Google are playing in the development of automated vehicles. Google's self-driving car program has been at the

[10] *Id*.
[11] *Id*.
[12] *See, e.g*., Testimony of Mary Louise Cummings, Director of Duke University's Humans and Autonomy Lab, Testimony Before the Senate Committee on Commerce, Science, and Transportation, *Hands Off: The Future of Self-Driving Cars* (Mar. 15, 2016), https://www.commerce.senate.gov/public/_cache/files/c85cb4ef-8d7f-40fb-968c-c476c5220a3c/8BC0CC7E137483CEFD0C928ECB14E74E.cummings-senate-testimony-2016.pdf ("[P]rivacy and control of personal data is also going to be a major point of contention. These cars carry cameras that look both in and outside the car, and will transmit these images and telemetry data in real time, including where you are going and your driving habits. Who has access to this data, whether it is secure, and whether it can be used for other commercial or government purposes has yet to be addressed.").
[13] Ellen P. Goodman, *Self-Driving Cars: Overlooking Data Privacy is a Car Crash Waiting to Happen*, THE GUARDIAN (June 8, 2016), https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security.
[14] Andy Sharman, *BMW Sounds Alarm Over Tech Companies Seeking Connected Car Data*, FINANCIAL TIMES (Jan. 14, 2015), https://www.ft.com/content/685fe610-9ba6-11e4-950f-00144feabdc0#axzz3PMmNVHKX.
[15] *Id*.

forefront of developing autonomous driving.[16] Google also earns nearly all of its profits by collecting and monetizing the personal data of consumers. And Google recently changed its privacy policy to combine consumers' web browsing history with their personally identifiable information, reversing course on the company's previous commitment to keep online ad tracking anonymous.[17]

Self-driving cars bring to mind the vehicles deployed by Google as part of the "StreetView" project. These camera-equipped cars captured not only digital imagery but also recorded WiFi hotspot locations and intercepted local WiFi communications, including "personal emails, usernames, passwords, videos, and documents."[18] In other words, vehicles connected to the Internet were intercepting and storing private WiFi transmissions, obtained from residential networks. Google later discontinued this practice after it was discovered, despite the company's attempts to conceal this egregious privacy invasion.[19] The Google StreetView example is a cautionary tale for the development of automated vehicles, which have even greater sensory technologies, capable of capturing electronic communications, digital imagery, radar mapping, audio communications, and even facial recognition.[20]

---

[16] Tim Higgins, *Google's Self-Driving Car Program Odometer Reaches 2 Million Miles*, WALL ST. J. (Oct. 5, 2016), http://www.wsj.com/articles/googles-self-driving-car-program-odometer-reaches-2-million-miles-1475683321 ("Google's self-driving car program Wednesday marked more than 2 million miles driven on public roads, a significant lap around traditional auto makers' efforts to develop autonomous vehicles.").

[17] Suzanne Monyak, *Google Changed a Major Privacy Policy Four Months Ago, and No One Really Noticed*, SLATE (Oct. 21, 2016), http://www.slate.com/blogs/future_tense/2016/11/11/facebook_will_no_longer_allow_advertisers_to_target_some_ads_by_race.html.

[18] *Joffe v. Google, Inc.*, 746 F.3d 920, 923 (9th Cir. 2013); *see* EPIC, *Investigations of Google Street View* (2015), https://epic.org/privacy/streetview.

[19] *See, e.g., In re: Google, Inc. Street View Electronic Communications Litigation*, No. 3:2010-md-02184 (N.D. Cal.); Sarah Gray, *Google Must Now Face Lawsuit Over Street View Privacy Invasion*, SALON (June 30, 2014), http://www.salon.com/2014/06/30/google_must_now_face_lawsuit_over_street_view_privacy_invasion/.

[20] Other techniques include "LIDAR" (Light Detection and Ranging) which generates enhanced imaging but also requires more processing. *See* Cade Metz, *Laser Breakthrough Could Speed the Rise of Self-*

Car manufacturers briefly inform consumers of data collection practices.[21] These notices fail to inform consumers about the true scope of data collection, and none give consumers true control over their data. Although some manufacturers allow consumers to delete already recorded data, preventing the car from constantly collecting and transmitting new data will often require "disabling valuable vehicle features or services."[22] In addition, car manufacturers use personal driving information for various but vague purposes, which leaves consumers in the dark about who has access to their information and why.[23] Personal driving information is often retained for years, if not indefinitely.[24]

Data generated by connected car technologies have a significant potential for secondary uses. Where car manufacturers and service providers are collecting and retaining information simply because they can, the ability of law enforcement to access this data could create entirely new and highly attractive methods of domestic surveillance. Drivers also risk having their sensitive driving and vehicle data disclosed or sold to unknown third parties for marketing purposes.

The ability of cars to generate, store, and transmit sensitive driving information has also led to the development of "Usage-Based Insurance" ("UBI").[25] UBI allows car insurance companies to set premiums based on a driver's mileage and driving behavior.[26] Although UBI currently accounts for a small percentage of insurance policies, the market for sensitive driving information is growing and by 2020 it is expected that 36 percent of all car insurance carriers will

---

Driving Cars, WIRED (Sept. 3, 2015), https://www.wired.com/2015/09/laser-breakthrough-speed-rise-self-driving-cars/.

[21] Markey Report at 12.

[22] *Id*.

[23] *Id*. at 11.

[24] *Id*.

[25] *Usage-Based Insurance & Telematics*, Nat'l Ass'n of Ins. Comm'rs (Oct. 8, 2015), http://www.naic.org/cipr_topics/topic_usage_based_insurance.htm.

[26] *Id.*

be using UBI.[27] The actuarial interest in detailed driving information will only grow, particularly as the growing automated vehicle industry facilitates more granular data collection.

B. Inadequate Data Security Within Networked Vehicles Can Pose Serious Risks of Physical Injury and Privacy Harms

In addition to privacy concerns, networked vehicles also raise serious safety concerns. Nearly all cars on the road today contain at least one wireless entry point ("WEP").[28] WEPs are essential to the functionality of built-in wireless features such as tire pressure monitoring systems, Bluetooth, keyless entry, anti-theft systems, and navigation.[29] However, WEPS also provide entry points for remote vehicle hacking. A 2011 report by computer scientists showed how a hacker could use WEPs to "take control of various features – like the car locks and brakes – as well as to track the vehicle's location, eavesdrop on its cabin and steal vehicle data."[30]

In a 2013 study, researchers Charlie Miler and Chris Valasek connected laptops to the computer systems of a Toyota Prius and a Ford Escape and were able to jerk the wheel at high speeds, turn the car, cause sudden acceleration or braking, turn on the horn, tighten the seatbelts in anticipation of a nonexistent crash, and kill the breaks.[31] In 2015, those same researchers were able to wirelessly hack a Jeep Cherokee traveling on a highway ten miles away from their computers.[32] The researchers were able to manipulate the air conditioning, turn on the radio,

---

[27] *Id.*
[28] Markey Report, *supra* note 9 at 5.
[29] *Id.*
[30] John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. Times (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html.
[31] Dr. Charlie Miller & Chris Valasek, *Adventures in Automotive Networks and Control Units*, IOActive (2014) http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf; Steve Henn, *With Smarter Cars, The Doors Are Open To Hacking Dangers*, NPR (July 30, 2013), http://www.npr.org/sections/alltechconsidered/2013/07/30/206800198/Smarte r-Cars-Open-New-Doors-To-Smarter-Thieves.
[32] 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-remotelykill-jeep-highway/.

activate the windshield wipers and wiper fluid, take over the car's digital display screen, cut the transmission, kill the engine, and engage and disable the breaks.[33] And earlier this year, those same researchers were able to control steering of the Jeep Cherokee and activate the safety brake while the vehicle was travelling at high speeds.[34]

While researches and scientists have done most of the reported hacks on moving cars in controlled setting, wide scale malicious car hacking is certainly imminent.[35] Thieves can already hack computer-based door lock systems to rob parked cars.[36] And in 2010, a disgruntled former car salesman disabled more than one hundred cars in Austin, Texas by hacking into a "web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments."[37]

The very real possibility of remote car hacking poses substantial risks to driver safety and security. Cars can be remotely hacked from anywhere in the world via the internet.[38] Wireless

[33] *Id*.
[34] Adam Greenberg, *The Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse*, WIRED, Aug. 1, 2016, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.
[35] *See, e.g*. Alex Hern, *Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking*, The Guardian (Sept. 7, 2015), http://www.theguardian.com/technology/2015/sep/07/fiat-chrysler-recalls- more-jeeps-wireless-hacking; Reem Nasr, *Fiat Chrysler recalling 1.4M vehicles amid hacking defense*, CNBC (July 24, 2015), http://www.cnbc.com/2015/07/24/fiat- chrysler-recalling-14m-vehicles-amid-hacking-defense.html; Miller & Valasek *supra* note 19.; Charlie Osborne & Zero Day, *Your Car Will Be Recalled in 2017 Thanks To Poor Open Source Security*, ZDNET, Nov. 21, 2016, http://www.zdnet.com/article/2017-the-year-hacking-will-force-your-car-to-be-recalled/.
[36] Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.
[37] Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, WIRED (Mar. 17, 2012), https://www.wired.com/2010/03/hacker-bricks-cars/.
[38] 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-remotelykill-jeep-highway/.

hacking can give hackers access to the cars physical location which would facilitate crimes such as harassment, stalking, and car theft.[39]

II. NHSTA SHOULD REQUIRE COMPLIANCE WITH THE CONSUMER PRIVACY BILL OF RIGHTS

EPIC supports NHTSA's recognition that automated vehicles raise privacy concerns, and backs the agency's endorsement of the Consumer Privacy Bill of Rights ("CPBR").[40] However, the Policy's recommendations for manufacturers' privacy policies fail to provide consumers with numerous essential rights under the CPBR and instead echoes a "notice and choice" framework.

A. NHTSA Must Fully Apply the Consumer Privacy Bill of Rights to Automated Vehicles

Drivers deserve basic privacy protections. Companies that collect and use personal information have an ongoing responsibility to those whose data they have collected. The starting point for a data protection framework is the Fair Information Practices ("FIPs").[41] The basic premise of the FIPs places responsibilities on entities collecting personal information and grants rights to individuals when their data is collected.

The Consumer Privacy Bill of Rights ("CPBR") is a significant formulation of the FIPs.[42] The CPBR grants consumers rights and places obligations on private companies collecting

---

[39] *Id*. *See also* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, MOTHERBOARD, Jul. 25, 2016, https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

[40] Nat'l Highway Traffic Safety Admin., *Federal Automated Vehicles Policy* (Sep. 2016), at 19 [hereinafter "Federal AV Policy"].

[41] EPIC, *The Code of Fair Information Practices*, https://www.epic.org/privacy/consumer/code_fair_info.html.

[42] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter White House, CPBR]; *see also White House Sets Out Consumer Privacy Bill of Rights*, EPIC, https://epic.org/privacy/white_house_consumer_privacy_.html.

consumer information. The CPBR offers seven technology-neutral practices for consumer privacy:

1. **Individual Control**: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
2. **Transparency**: Consumers have a right to easily understandable and accessible information about privacy and security practices.
3. **Respect for Context**: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
4. **Security**: Consumers have a right to secure and responsible handling of personal data.
5. **Access and Accuracy**: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
6. **Focused Collection**: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
7. **Accountability**: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[43]

The CPBR would help establish fairness and accountability for the collection and use of drivers' personal information. This framework would establish baseline safeguards for the development of innovative car technology while safeguarding individual privacy.

While NHTSA's privacy recommendations follow the practices enumerated in the CPBR, several key elements are undercut by reference to the manufacturer's privacy policy as the controlling document. For example, the "Respect for Context" principle would simply require use of driver data in ways that are consistent with the purposes for collection "as explained in applicable data privacy notice/agreements."[44] This reference to privacy policies is not found in the CPBR or the FIPs. Moreover, it would permit manufacturers to claim vague, overbroad collection purposes in order to use driver in virtually unlimited ways. Emphasizing notice or

[43] White House, CPBR.
[44] Federal AV Policy at 19.

disclosure favors the interests of businesses over consumers and fails to establish meaningful privacy safeguards.

Regarding the "Choice" principle, NHTSA must make it clear that automated vehicle manufacturers, dealers, and insurers cannot condition the provision of goods and services on consumers consenting to invasive privacy practices. For example, a pay-for-privacy scheme (*i.e.*, charging consumers more to keep their data private) could be highly coercive when offered by insurance companies or high risk lenders. NHTSA should also clarify that drivers own the data generated by autonomous vehicles. Control of individual data is implicit within the rights granted to consumers under the CPBR.

EPIC urges NHTSA to revise the Guidance with respect to manufacturers' privacy obligations in a manner consistent with the CPBR. Specifically, NHTSA should remove references to "data privacy notices/agreements" in order to restore substantive rights to consumers and limit carmakers' ability to hide behind incomprehensible privacy policies. Most importantly, NHTSA should promulgate mandatory, legally enforceable privacy rules for automated vehicle manufacturers. Voluntary codes of conduct and industry self-regulation simply cannot provide realistic privacy protections when they are not supported by enforceable legal standards.

B. The Auto Industry's Privacy Pledge Fails to Protect Driver Privacy

The NHTSA guidelines reference the "Privacy Principles for Vehicle Technologies and Services" published by the Alliance of Automobile Manufacturers and the Association of Global Automakers.[45] While the pledge is an important first step for the industry to recognize consumer

[45] Federal AV Policy at 19; Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, *Consumer Privacy Protection Principles for Vehicle Technologies and Services* (Nov, 12, 2014), http://www.autoalliance.org/auto-issues/automotive-privacy/principles.

privacy issues, it is no substitution for baseline privacy protections. NHTSA should require manufacturers to provide real, concrete privacy protections.

First, the industry principles are "subject to change over time," and do not directly apply to the countless third-party service providers with whom auto manufacturers contract to collect driver information or other businesses with whom consumers directly engage to receive services.[46] Second, the pledge is premised on auto manufacturers providing drivers with notice and choice about the types of information the manufacturers collect, use, and disclose. Pledge participants may provide drivers notice in any way participants choose, including in "owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays."[47] But pledge members have broad authority to change the ways in which they collect, use, and disclose driver information and have wide discretion as to whether they should inform drivers of any changes in their privacy policies.[48]

Although pledge members commit to obtaining driver consent before using or disclosing driver location information, biometrics, and driver behavior information for marketing, the pledge grants members authority to use and disclose this sensitive driver personal information without consent for several broad purposes, including "for internal research or product development" or with third-party service providers providing "vehicle technologies and

[46] *Id*. at 2, 3-4.
[47] *Id*. at 6.
[48] *Id*. at 6-7 ("Notices need not be provided prior to every instance of collection where addressed by prior notices." "Participating Members commit to taking reasonable steps to alert Owners and Registered Users prior to changing the collection, use, or sharing practices associated with Covered Information in ways that have a material impact on Owners or Registered Users.").

services."[49] The pledge even permits auto manufacturers to sell driver information pursuant to a company merger or acquisition.[50]

The constraints on the amount of data collected and how long auto manufacturers keep the information are unbounded: pledge participants can keep and store driver personal information as long as needed for "legitimate business purposes."[51] Although companies and their contractors collect a host of personal data, the pledge states that the members may provide drivers a way to correct and review only a limited subset of personal subscription information, like name, address, credit card numbers, telephone number or email address.[52] For other sensitive information like biometrics, members only commit to "exploring additional means" of providing drivers with "reasonable access" to their own driving information.[53] Notwithstanding the various exceptions and loopholes the pledge provides, the pledge lacks any meaningful oversight and accountability mechanisms. In sum, the pledge supports the status quo of wholesale collection of sensitive driver personal information and fails to provide essential privacy protections.

III. THE FEDERAL AUTOMATED VEHICLES POLICY MUST INCLUDE MEANINGFUL OVERSIGHT AND ENFORCEMENT MECHANISMS

The Federal Automated Vehicles Policy is a step toward protecting driver privacy. However, the Policy is voluntary and is missing oversight and enforcement mechanisms. Automotive vehicle manufacturers are given a range of things that they *should* do, but not that they *must* do. Leaving essential privacy and security protections to the discretion of carmakers and

[49] *Id*. at 8-9. "Vehicle technologies and services" is broadly defined as "[t]echnologies and services provided by, made available through, or offered on behalf of Participating Members that involve the collection, use, or sharing of information that is collected, generated, recorded, or stored by a vehicle."
[50] *Id*. at 9.
[51] *Id*. at 11.
[52] *Id*.
[53] *Id*.

companies such as Google places consumers at risk. EPIC urges NHTSA to implement mandatory privacy protections for automated vehicles as soon as possible.

The Automated Vehicles Policy states that any disclosure of data to third parties "should not contain any personally identifiable information."[54] However, consumers have no recourse if the Policy is violated. Similarly, the Policy states that cybersecurity practices "should be fully documented…and data should be traceable within a robust document version control environment."[55] But there is no mechanism for enforcement.

The Automated Vehicles Policy should include meaningful oversight and enforcement mechanisms. NHTSA and the Department of Transportation ("DOT") should enforce privacy safeguards and security standards for automated vehicles.

Meaningful enforcement of privacy and security protections also requires a private right of action against companies who misuse and fail to secure personal information. Private rights of actions are familiar remedies in U.S. privacy law and would be appropriate in the context of automated vehicles.[56]

IV. NHTSA SHOULD ABANDON EFFORTS TO PREEMPT STATE LAW

EPIC strongly urges the NHTSA to abandon its efforts to preempt state law, especially as it relates to privacy protections for automated vehicles. As the Policy currently notes, the Vehicle Safety Act preempts states from issuing any standard that regulates vehicle performance if the standard is not identical to an existing Federal Motor Vehicle Safety Standard ("FMVSS") that regulates that same aspect of performance.[57] Historically, federal privacy laws have not preempted

[54] Federal AV Policy at 18.
[55] *Id.* at 21
[56] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692–1692p; Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508; 100 Stat. 1848.
[57] Federal AV Policy at 38.

stronger state law protections or enforcement mechanisms. In both the privacy and consumer protection context, federal regulations serve as baselines while allowing states to enact and enforce stronger laws.[58]

While the federal government has enacted privacy laws, more robust privacy legislation has been implemented at the state level. Many states have enacted privacy legislation that exist alongside federal law covering the same material. Furthermore, under *Hillsborough County v. Automated Medical Laboratories* there is currently a presumption that state and local governments are primarily responsible for matters related to health and safety.[59] Privacy is included in the area of health and safety regulations that are traditionally left to the states.[60]

Seventeen states have already passed laws regarding privacy aspects of connected cars as it relates to event data recorders ("EDRs").[61] EDRs are devices that can record, retain, and report data related to drivers' operation of an automobile. The data stored can also be accessed by third parties. Several states have limited when EDR data can be accessed or require the driver's consent. Virginia, for example, prohibits insurance companies from reducing coverage, increasing premiums, applying surcharges, or denying discounts solely because a vehicle operator or owner refuses to grant her insurance company access to EDR data.[62] And Arkansas

---

[58] *See e.g.* Electronic Communications Privacy Act; Right to Financial Privacy Act; Cable Communications Privacy Act; Video Privacy Protection Act; Employee Polygraph Protection Act; Telephone Consumer Protection Act; Driver's Privacy Protection Act; Gramm-Leach-Bliley Act.
[59] *Hillsborough County v. Automated Medical Laboratories*, 471 U.S. 707 (1985).
[60] *See e.g. Hill v. Colorado*, 530 U.S. 703 (2000) (upholding a law that protected the privacy and autonomy of individuals seeking medical care because the law was intended to serve the traditional exercise of State police power to protect the health and safety of its citizens).
[61] Ark. Code § 23-112-107; Cal. Veh. Code § 9951; Colo. Rev. Stat. § 12-6-401, -402, -403; Conn. Gen. Stat. § 14-164aa; Del. Code § 3918; Me. Rev. Stat. Ann. tit. 29-A §§ 1971, 1972, 1973; Mont. Code § 61-12-1001 et seq.; Nev. Rev. Stat. § 484D.485; N.H. Rev. Stat. § 357-G:1; N.J. Stat. § 39:10B-7 et seq.; N.Y. Veh. & Traf. Code § 416-b; N.D. Cent. Code § 51-07-28; Or. Rev. Stat. § 105.925 et seq.; Tex. Transp. Code § 547.615; Utah Code § 41-1a-1501 et seq.; Va. Code §§ 38.2-2212(C)(s), 38.2-2213.1, 46.2-1088.6, 46.2-1532.2; Wash. Rev. Code §46.35.010.
[62] Va. Code Ann. § 38.2-2213.1 (West).

prohibits insurance companies from requiring EDR data access as a condition of an insurance policy.[63] Connecticut law requires law enforcement to obtain search warrants before accessing EDR data without owner consent.[64]

In addition, NHTSA would benefit from allowing states to play a role in crafting privacy regulations as automated vehicle technology advances. States have a unique perspective allowing them to develop innovative programs to protect consumers. As automated vehicle technology evolves, the states should be allowed to operate as laboratories of democracy – a role they have traditionally held in the field of privacy.[65] State legislatures are closer to their constituents and the entities that they regulate. Because states are often the first to recognize trends and emerging problems, and are well suited to address new challenges and opportunities as they arise and as technology evolves.

Allowing the states to contribute to the development and deployment of connected cars would allow them test certain areas that may be missed at the federal level and by the manufacturers themselves. For example, the California Department of Motor Vehicles recently released a plan that would compel manufacturers to address privacy and safety concerns as they relate to connected cars. The plan would require manufacturers to complete a 15-point report on safety and other issues before testing the cars or allowing them to operate on public roads.[66]

---

[63] Ark. Code Ann. §23-112-107 (West).
[64] Conn. Gen. Stat. Ann §14-164aa (West).
[65] *Hill v. Colorado,* 530 U.S. 703, 715 (2000) (upholding a law protecting the privacy and autonomy of individuals seeking medical care, as the law was intended to serve the "traditional exercise of the States' 'police powers to protect the health and safety of their citizens'").
[66] Brian Fung, *Federal Officials Take Aim at California's Plan For Self-Driving Cars*, WASH. POST, Nov. 15, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/11/15/federal-officials-are-mad-at-california-for-misuing-their-idea-on-self-driving-cars/.

V. CONCLUSION

EPIC is encouraged that NHTSA has acknowledged the privacy implications of automated vehicles and the utility of the Consumer Privacy Bill of Rights. However, EPIC urges the agency to meaningfully address the privacy challenges that will only become more complex as the automated vehicle industry advances. This requires enforceable privacy and security rules, not voluntary guidelines and industry self-regulation. Additionally, NHTSA must implement strong oversight mechanisms to ensure the future of driverless vehicles benefits consumers without placing their privacy rights and physical safety at risk. Finally, NHTSA should not preempt state laws that provide stronger privacy protections, building on federal baseline requirements.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Claire Gartland
Claire Gartland
Director, EPIC Consumer Privacy Project

/s/ Kimberly Miller
Kimberly Miller
EPIC Administrative Law Fellow