epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 13, 2017

The Honorable John Thune, Chairman
The Honorable Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce, Science & Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on "Paving the Way for Self-Driving Vehicles"

Dear Chairman Thune and Ranking Member Nelson:

We write to your regarding the upcoming hearing "Paving the Way for Self-Driving Vehicles,"[1] on the privacy and safety risks of connected and autonomous vehicles. For more than a decade, the Electronic Privacy Information Center ("EPIC") has warned federal agencies and Congress about the growing risks to privacy resulting from the increasing collection and use of personal data concerning the operation of motor vehicles.[2]

EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC engages in a wide range of public policy and litigation activities. EPIC testified before the House of Representatives in 2015 on "the Internet of Cars."[3] Recently, EPIC

[1] *Paving the Way for Self-Driving Vehicles*, 115th Cong. (2017), S. Comm. on Commerce, Science, and Transportation, https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=B7164253-4A43-4B70-8A73-68BFFE9EAD1A (June 14, 2017).

[2] *See generally* EPIC, "Automobile Event Data Recorders (Black Boxes) and Privacy," https://epic.org/privacy/edrs/. *See also* EPIC, Comments, Docket No. NHTSA-2002-13546 (Feb. 28, 2003), *available at* https://epic.org/privacy/drivers/edr_comments.pdf ("There need to be clear guidelines for how the data can be accessed and processed by third parties following the use limitation and openness or transparency principles."); EPIC, Comments on Federal Motor Vehicle Safety Standards; V2V Communications, Docket No. 2016-0126 (Apr. 12, 2017), https://epic.org/apa/comments/EPIC-NHTSA-V2V-Communications.pdf [hereafter "V2V comments"]; EPIC, Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Docket No. 160331306-6306-01 (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf; EPIC, Comments on Federal Motor Vehicle Safety Standards: "Vehicle-to-Vehicle (V2V) Communications," Docket No. NHTSA-2014-0022 (Oct. 20, 2014), https://epic.org/privacy/edrs/EPIC-NHTSA-V2V-Cmts.pdf; EPIC, Comments on the Privacy and Security Implications of the Internet of Things (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf; EPIC et al., Comments on the Federal Motor Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177 (Feb. 11, 2013), https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf; EPIC, Comments, Docket No. NHTSA-2004-18029 (Aug. 13, 2004); https://epic.org/privacy/drivers/edr_comm81304.html.

[3] Statement of Khaliah Barnes, hearing on *The Internet of Cars* before the House Committee on Oversight and Government Reform, November 18, 2015, https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.

urged the Ninth Circuit of Appeals to protect the right of consumers to pursue safety issues with connected vehicles.[4] As EPIC explained in that case:

> "Connected vehicles" expose American drivers to the risks of data breach, auto theft, and physical injury. The internal computer systems for these vehicles are subject to hacking, unbounded data collection, and broad-scale cyber attack. Despite this extraordinary risk, car manufacturers are expanding the reach of networked vehicles that enable third party access to driver data and vehicle operational systems.[5]

EPIC will also be participating in the FTC/NHTSA workshop on privacy and security issues in connected cars later this month.[6]

Connected vehicles pose substantial safety and privacy risks. To date there have been several high-profile accidents involving self-driving car including:

- A bicyclist was struck by an autonomous driving car after it suddenly activated its brakes;[7]
- Uber recently suspending its "self-driving" program in Arizona after one of the company's vehicles struck a car with passengers inside.[8] The Uber vehicle was in self-driving mode, presumably "Level 3";
- A self-driving car failed to stop at a red light at a busy intersection;[9] and
- A Tesla owner was recently involved in an accident when the autopilot failed recognize a lane shift in a construction zone, resulting in a collision with a construction barrier.[10]

These accidents should alarm the Committee and the public, but they are only one of myriad issues with autonomous vehicles. Wide-scale malicious automobile hacking is no longer

---

[4] 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.
[5] *Id.*
[6] *Connected Cars: Privacy, Security Issues Related to Connected Automated Vehicles,* Federal Trade Commission, https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.
[7] Patrick May, *Robot-Human Smackdown: Self-Driving Car and Bicyclist Collide in San Francisco*, The Mercury News, Jun. 9, 2017, http://www.mercurynews.com/2017/06/09/robot-human-smackdown-self-driving-car-and-bicyclist-collide-in-san-francisco/.
[8] Mike Isaac, *Uber Suspends Tests of Self-Driving Vehicles After Arizona Crash*, New York Times, Mar. 25, 2017, https://www.nytimes.com/2017/03/25/business/uber-suspends-tests-of-self-driving-vehicles-after-arizona-crash.html; Steven Overly, *Uber Self-Driving Car Flipped On Side In Arizona Crash*, Chicago Tribune, Mar. 25, 2017, http://www.chicagotribune.com/bluesky/technology/ct-uber-self-driving-car-crash-20170325-story.html.
[9] Mike Isaac & Daisuke Wakabayashi, *A Lawsuit Against Uber Highlights the Rush to Conquer Driverless Cars*, New York Times, Feb. 24, 2017, https://www.nytimes.com/2017/02/24/technology/anthony-levandowski-waymo-uber-google-lawsuit.html.
[10] Antti Kautonen, *Tesla Driver Blames Autopilot for Barrier Crash*, Autoblog, Mar. 3, 2017, http://www.autoblog.com/2017/03/03/tesla-autopilot-barrier-crash/.

theoretical.[11] Although a full-scale remote car hijacking is certainly a serious risk to car owners and others,[12] hijacking is not the only risk posed by connected car vulnerabilities.[13] Connected cars leave consumers open to car theft, data theft, and other forms of attack as well. These attacks are not speculative; many customers have already suffered due to vulnerable car systems. For example, criminals have exploited vulnerabilities in connected cars to perpetrate car "ransomware" scams, "where a car is disabled by malicious code until a ransom is paid."[14]

Car manufacturers must adopt data security measures. Early mitigation of threats to public safety may reduce auto fatalities, spur innovation, and result in safer vehicles.[15] There should be great concern that each of autonomous car maker wants to be the first to have their vehicle available to the public can poses substantial safety risks.[16] A functioning autonomous vehicle does not mean security and the race to be the first with a functioning, marketable autonomous vehicle jeopardizes the safety and security of consumers.

Recently, Charlie Miller, whose research led Chrysler to recall 1.4 million vehicles after he hacked into a Jeep,[17] stated the danger in self-driving ridesharing and taxi services stating that "Autonomous vehicles are at the apex of all the terrible things that can go wrong. . . Cars are already insecure, and you're adding a bunch of sensors and computers that are controlling them. . . If a bad guy gets control of that, it's going to be even worse."[18] The potential risks that connected cars pose to the driver, as well as the potential risk to the public, cannot be understated.

---

[11] Brief of *Amicus Curiae* EPIC, *Cahen v. Toyota Motor Corporation*, No. 16-15496 (9th Cir. Aug. 5, 2016), *available at* https://epic.org/amicus/cahen/EPIC-Amicus-Cahen-Toyota.pdf.
[12] *See, e.g.*, 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/.
[13] *See* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, Motherboard (July 25, 2016), http://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster (explaining that information systems face three threats: theft (i.e. loss of confidentiality), modification (i.e. loss of integrity), and lack of access (i.e. loss of availability)).
[14] Nora Young, *Your Car Can be Held for Ransom*, CBCradio (May 22, 2016), http://www.cbc.ca/radio/spark/321-life-saving-fonts-ransomware-cars-and-more-1.3584113/your-car-can-be-held-for-ransom-1.3584114.
[15] *See generally*, Ralph Nader, *Unsafe at Any Speed* (1965).
[16] Mike Isaac, *Lyft and Waymo Reach Deal to Collaborate on Self-Driving Cars,* New York Times, May 14, 2017, https://www.nytimes.com/2017/05/14/technology/lyft-waymo-self-driving-cars.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=sectionfront; Alex Davies, *Detroit Is Stomping Silicon Valley in the Self-Driving Car Race,* Wired, Apr. 3, 2017, https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/.
[17] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 Million Vehicles for Bug Fix,* Wired, Jul 24, 2015, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/; Andy Greenberg, *Hackers Remotely Kill A Jeep on the Highway—With Me In It,* Wired, Jul. 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Andy 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/.
[18] Andy Greenberg, *Securing Driverless Cars From Hackers Is Hard. Ask The Ex-Uber Guy Who Protects Them*, Wired, Apr. 12, 2017, https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.

In paving the way for the development and deployment of self-driving cars this Committee should be aware of the National Highway Traffic Safety Administration's recent proposals that would pre-empt states from being involved in this process. Historically, federal privacy laws have not preempted strong state protections or enforcement mechanisms.[19] However, NHTSA recently proposed issuing a new Federal Motor Vehicle Safety Standard for vehicle-to-vehicle communications[20] and the Federal Automated Vehicle Policy envisions NHTSA issuing FMVSS's as connected cars are developed.[21] However, under the Vehicle Safety Act the states are pre-empted from issuing any standards for vehicle performance if it is not identical to an existing FMVSS that regulates the same aspect of performance.[22] As EPIC recently explained to the NHTSA:

> States have a unique perspective allowing them to develop innovative programs to protect consumers. As [connected car] technology evolves, the states should be allowed to operate as laboratories of democracy—a role they have traditionally held in the field of privacy.[23]

The Committee must make clear that the states must continue to have the same pivotal role for developing privacy regulations that they have traditionally held.

EPIC urges this Committee to take these accidents and security flaws into account as it examines the future of transportation as it relates to these vehicles. In addition to the substantial privacy concerns that connected cars present,[24] these recent incidents show that there are substantial safety concerns to everyone on the road. *National minimum standards for safety and privacy are needed to ensure the safe deployment of connected vehicles.*

Auto manufacturers have a particular responsibility to ensure the safety of drivers. Mr. Mitch Brainwol from the Alliance of Automobile Manufacturers should be asked:

- What are automobile manufacturers doing to ensure data security in connected cars?

Mr. Rob Csongor from NVIDIA Corporation should be asked:

---

[19] *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.
[20] *Federal Motor Vehicle Safety Standards; V2V Communications,* 82 Fed. Reg. 3,854 (Jan. 12, 2017).
[21] Nat'l Highway Traffic Safety Admin., *Federal Automated Vehicles Policy* (Sep. 2016).
[22] "When a motor vehicle safety standard is in effect under this chapter, a State or a political subdivision of a State may prescribe or continue in effect a standard applicable to the same aspect of performance of a motor vehicle or motor vehicle equipment only if the standard is identical to the standard prescribed under this chapter." 49 U.S.C. § 30102(b)(1).
[23] V2V comments at 10.
[24] 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; Jeff John Roberts, *Watch Out That Your Rental Car Doesn't Steal Your Phone Data,* Fortune, Sep. 1, 2016, http://fortune.com/2016/09/01/rental-cars-data-theft/.

- What information is NVIDIA collecting on drivers?
- What is NVIDIA doing to secure driver data?
- What cybersecurity measures has NVIDIA adopted to minimize the risk that its cars can be hacked?

We ask that this Statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Kim Miller
Kim Miller
EPIC Policy Fellow