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

May 17, 2017

The Honorable Mario Diaz-Balart, Chairman
The Honorable David Price, Ranking Member
U.S. House of Representatives Committee on Appropriations
Subcommittee on Transportation, Housing and Urban Development, and Related Agencies
2358-A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Diaz-Balart and Ranking Member Price:

We write to your regarding the upcoming hearing "Emerging Transportation Technologies,"[1] on the privacy and safety risks of "connected vehicles." For more than a decade, EPIC has warned federal agencies and the Congress about the growing risks to privacy resulting from the increasing collection and use of personal data concerning the operation of motor vehicles.[2] In recent years, we have become increasingly aware of the threat to public safety of Internet-connected vehicles.[3]

Connected vehicles pose substantial safety and privacy risks. To date there have been several high-profile accidents involving self-driving cars. For example, Uber recently suspended

[1] *Emerging Transportation Technologies* before the House Committee on Appropriations, Subcommittee on Transportation, Housing and Urban Development, and Related Agencies, http://appropriations.house.gov/calendar/eventsingle.aspx?EventID=394869.

[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 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), *available at* 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), *available at* 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), *available at* 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), *available at* https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf; EPIC, Comments, Docket No. NHTSA-2004-18029 (Aug. 13, 2004); *available at* https://epic.org/privacy/drivers/edr_comm81304.html.

[3] Testimony of EPIC Associate Director Khaliah Barnes, hearing on the *Internet of Cars* before the House Committee on Oversight and Government Reform, Nov. 18, 2015, https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf; Statement of EPIC, hearing on *Self-Driving Cars: Road to Deployment* before the House Committee on Energy and Commerce, Subcommittee on Digital Commerce & Consumer Protection, Feb. 14, 2017, http://docs.house.gov/meetings/IF/IF17/20170214/105548/HHRG-115-IF17-20170214-SD012.pdf.

its "self-driving" program in Arizona after one of the company's vehicles struck a car with passengers inside.[4] The Uber vehicle was in self-driving mode, presumably "Level 3." The accident with the Uber vehicle highlights the risks of the "self-driving" mode as well as the dangers of having these vehicles on the road with traditional vehicles.

This is not the first accident involving an autonomous vehicle. Late last year, a self-driving car failed to stop at a red light at a busy intersection.[5] 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.[6]

These accidents should alarm the Subcommittee and the public, but they are only one of myriad issues with autonomous vehicles. Wide-scale malicious automobile hacking is no longer theoretical.[7] Although a full-scale remote car hijacking is certainly a serious risk to car owners and others,[8] hijacking is not the only risk posed by connected car vulnerabilities.[9] 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."[10] According to one expert, computer criminals have installed malicious software in cars via USB drives used by mechanics for diagnostics and software updates. The software shuts down, or "bricks," the car unless and until the driver meets the criminal's demands. The expert even discovered a case where an entire fleet of vehicles was disabled by ransomware. She warns that criminals can also infect a car with malware remotely over the car's wireless connection.[11]

---

[4] 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.

[5] Mike Isaac & Daisuke Wakabyashi, *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.

[6] Antti Kautonen, *Tesla Driver Blames Autopilot for Barrier Crash*, Autoblog, Mar. 3, 2017, http://www.autoblog.com/2017/03/03/tesla-autopilot-barrier-crash/.

[7] 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.

[8] *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/.

[9] *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)).

[10] 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.

[11] *Id.*

Car manufacturers should adopt data security measures. Early mitigation of threats to public safety may reduce auto fatalities, spur innovation, and result in safer vehicles.[12] 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.[13] 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, 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."[14] The potential risks that connected cars pose to the driver, as well as the potential risk to the public, cannot be understated.

EPIC urges this Subcommittee 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,[15] 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.

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

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Kim Miller
Kim Miller
EPIC Policy Fellow

[12] *See generally*, Ralph Nader, *Unsafe at Any Speed* (1965).
[13] 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/.
[14] 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/.
[15] 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/.