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

March 27, 2017

The Honorable Robert Latta, Chairman
The Honorable Janice Schakowsky, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Digital Commerce & Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Latta and Ranking Member Schakowsky:

For today's hearing on "Self-Driving Cars: Levels of Automation,"[1] we write to you again regarding the privacy and safety risks of self-driving 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]

This past weekend, Uber suspend the company's self-driving cars program in Arizona after one of their vehicles was in an accident with a traditional car in Arizona.[4] The Uber vehicle,

---

[1] *Self-Driving Cars: Levels of Automation* before the House Committee on Energy & Commerce, Subcommittee on Digital Commerce and Consumer Protection, https://energycommerce.house.gov/hearings-and-votes/hearings/self-driving-cars-levels-automation.

[2] 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] Statement of 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.

[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-

had a person in the driver's seat but 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 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]

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]

---

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.*

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

EPIC urges this subcommittee to take these accidents and security flaws into account as you examine the various levels of automation in these vehicles. In addition to the substantial privacy concerns that these new cars present,[13] these recent incidents show that there are substantial safety concerns to everyone on the road.

Several states have recognized the risks to their residents and have passed laws regulating connected vehicles.[14] But consumer nationwide deserve protection. National minimum standards for safety and privacy are needed to ensure the safe deployment of connected vehicles.

We ask that this letter 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

[13] 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/.

[14] Nat'l Highway Traffic Safety Admin., Federal Automated Vehicles Policy (Sep. 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf ; 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).