



February 13, 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

**RE: Hearing on “Self-Driving Cars: Road to Deployment”**

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the upcoming hearing on connected vehicles.<sup>1</sup> New vehicle technologies are being quickly implemented by car manufacturers. But these new technologies also raise serious safety and privacy concerns that Congress needs to address. Current approaches, based on industry self-regulation, are inadequate and fail to protect driver privacy and safety. Increased congressional oversight is imperative, as this fast-evolving industry affects the safety and privacy of millions of Americans.

The Electronic Privacy Information Center 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 this Committee in 2015 on “the Internet of Cars.”<sup>2</sup> While we appreciate that legislation was adopted subsequently to gather data on the privacy impact of connected vehicles, we believe more should be done.<sup>3</sup> Recently, EPIC urged the Ninth Circuit of Appeals to protect the right of consumers to pursue safety issues with connected vehicles.<sup>4</sup>

---

<sup>1</sup> *Self-Driving Cars: Road to Deployment* before the House Committee on Energy & Commerce, <https://energycommerce.house.gov/hearings-and-votes/hearings/self-driving-cars-road-deployment>.

<sup>2</sup> 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>.

<sup>3</sup> Driver Privacy Protection Act of 2015.

<sup>4</sup> Brief of *Amicus Curiae* EPIC, *Cahen v. Toyota Motor Corporation*, No. 16-15496 (9th Cir. Aug. 5, 2016), <https://www.epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf>.

“Connected cars” are connected to the Internet, which creates safety and privacy risks. For example, researchers have already been able to hack into and take control of connected cars.<sup>5</sup> Furthermore, cars with telematics transmits location data from a car and a service provider.<sup>6</sup> This leads to the collection of vast amounts of location information that exposes extensive private information on driver habits such as where a driver lives and works or where they go on a Friday night.<sup>7</sup>

Many consumers who rent vehicles are also confronting bluetooth enabled systems that collect their entire address books from their cellphones.<sup>8</sup> This also raises serious privacy concern.<sup>9</sup>

The recent trend by federal agencies to issue voluntary guidance and allow manufacturers to self-regulate is not working.<sup>10</sup> While this guidance is a helpful starting point, consumers would be safer if there were concrete minimum safety and privacy requirements for connected cars.

A nationwide standard is needed to ensure the safe deployment of connected vehicles. Currently, several states have adopted laws for connected vehicles, but they vary from state to

---

<sup>5</sup> 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](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/Smarter-CarsOpen-New-Doors-To-Smarter-Thieves>; 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-remotelykill-jeep-highway/>; Bruce Schneier, *Hackers Stealing Cars*, *Schneier on Security*, Aug. 11, 2016, [https://www.schneier.com/blog/archives/2016/08/hackers\\_stealin.html](https://www.schneier.com/blog/archives/2016/08/hackers_stealin.html); Bruce Schneier, *Autonomous Vehicles as Bombs*, *Schneier on Security*, Oct. 6, 2015, [https://www.schneier.com/blog/archives/2015/10/autonomous\\_vehi.html](https://www.schneier.com/blog/archives/2015/10/autonomous_vehi.html).

<sup>6</sup> 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>.

<sup>7</sup> *Id.* at 2

<sup>8</sup> Lisa Weintraub Schifferle, *What Is Your Phone Telling Your Rental Car?*, Federal Trade Commission, Aug. 30, 2016, <https://www.consumer.ftc.gov/blog/what-your-phone-telling-your-rental-car>; Cale Guthrie Weissman, *Watch Out For This Incredibly Easy Way That Rental Cars Can Intercept Your Smartphone Data*, *Business Insider*, Jul. 6, 2015, <http://www.businessinsider.com/rental-car-bluetooth-hands-free-devices-can-intercept-your-smartphone-data-2015-7>.

<sup>9</sup> 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/>; Bruce Schneier, *Tracking Connected Vehicles*, *Schneier on Security*, Oct. 29, 2015, [https://www.schneier.com/blog/archives/2015/10/tracking\\_connec.html](https://www.schneier.com/blog/archives/2015/10/tracking_connec.html) (“Researchers have shown that it is both easy and cheap to surveil connected vehicles.”)

<sup>10</sup> 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>

state.<sup>11</sup> Consumers nationwide deserve these protections. A national minimum standard is needed. Stronger privacy safeguards should also be established.

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

---

<sup>11</sup> 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).