epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

January 12, 2017

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

RE: Nomination hearing for Elaine Chao: Drones and Connected Vehicles

Dear Chairman Thune and Ranking Member Nelson:

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has taken a particular interest in the unique privacy problems of Unmanned Aerial Vehicles (UAVs or "drones"), and has sued the FAA for its failure to establish privacy safeguards to protect Americans.[1] EPIC has also testified before Congress regarding the privacy and data security implications of autonomous vehicles.[2]

Chairman Thune noted yesterday that drones and autonomous vehicles are two significant issues facing the next Secretary of Transportation. EPIC agrees. Specifically,

[1] *EPIC v. FAA*, No. 15-1075 (D.C. Cir. Filed Mar. 31, 2015); *See also Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, https://epic.org/privacy/drones/; *See also* EPIC, *EPIC v. FAA, Challenging the FAA's Failure to Establish Drone Privacy Rules,* https://epic.org/privacy/litigation/apa/faa/drones/

[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. *See also* Marc Rotenberg, A*re Vehicle Black Boxes a Good Idea?* Costco 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.

1. The FAA Should Establish Comprehensive Privacy Rules for Drones.

Drones pose a unique threat to the privacy of Americans. These small, autonomous devices routinely record images of people and have the ability to track people and even record private communications.[3] The 2012 FAA Act made clear that the FAA was to undertake a "comprehensive plan," including privacy safeguards, prior to permitting the deployment of commercial drones in US national airspace. Moreover, more than one hundred experts and organizations have petitioned the FAA to establish a privacy rule. Yet, the agency has failed to fulfill its statutory obligations or to follow the advice of experts.

2. There Should Be Comprehensive Privacy Laws and Safety Mandates for Connected Vehicles

Connected vehicles, now on the streets in the United States, raise substantial privacy risks. Connected cars collect and broadcast troves of sensitive personal data. This data can be used for many purposes unrelated to the operation of the vehicle, including tracking, marketing, stalking, and surveillance. Last year, Congress enacted legislation, based on this Committee's work, that begin address these issues, but far more needs to be done.[4]

Connected vehicles also raise significant safety concerns within the broader Internet of Things, an ever-expanding network of devices, people, and machines.[5] Cars make up a significant segment of the network, with vehicle technologies offering consumer services such as on-board navigation and tire pressure monitoring. But autonomous cars have hidden risks much like the camera-equipped Google "StreetView" cars that captured not only digital imagery but also recorded WiFi hotspot locations and intercepted local WiFi communications, including "personal emails, usernames, passwords, videos, and documents."[6] There is also the risk of remote hacking, an ever increasing risk as more of a vehicle's functionality is connected to the network.[7]

Current policy approaches, based on industry self-regulation, fail to protect driver privacy and safety. EPIC recently expressed our concerns to the NHTSA and urged the agency to issue

---

[3] *See, e.g.*, *Crimes – Unmanned Aircraft Systems – Unauthorized Surveillance, Hearing on H.D. 620 Before the H. Jud. Comm. of the General Assembly of Maryland* (2015) (statement of Jeramie D. Scott, National Security Counsel, EPIC); *The Future of Drones in America: Law Enforcement and Privacy Considerations Hearing Before the S. Judiciary Comm.*, 113th (2013) (statement of Amie Stepanovich, Director of the Domestic Surveillance Project, EPIC), *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf.

[4] Driver Privacy Act of 2015. S. 766, 114th Congress (2015).

[5] *Internet of Things*, EPIC, https://epic.org/privacy/internet/iot/ (last visited January 12, 2017).

[6] *Joffe v. Google, Inc.*, 746 F.3d 920, 923 (9th Cir. 2013); see *Investigations of Google Street View*, EPIC, https://epic.org/privacy/streetview (last visited Jan. 12, 2017).

[7] *See* EPIC, *Cahen v. Toyota Motor Corporation: Whether drivers can sue for privacy and security vulnerabilities in connected car, ht*tps://epic.org/amicus/cahen/

mandatory rules to address the myriad risks posed to drivers operating connected vehicles in the United States.[8]

Drones and autonomous cars are two of the most pressing issues facing the next Transportation Secretary. We appreciate the Committee's interest in these issues.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Senate Commerce Committee going forward.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Kimberly Miller
Kimberly Miller
EPIC Policy Fellow

[8] *EPIC Comments on the Federal Automated Vehicles Policy*, Nov. 22, 2016, https://epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf.