epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Khaliah Barnes
Associate Director and Administrative Law Counsel, EPIC

Hearing on

"The Internet of Cars"

Joint Hearing Before the

U.S. House of Representatives,
Committee on Oversight and Government Reform
Subcommittee on Information Technology and
Subcommittee on Transportation and Public Assets

November 18, 2015
2154 Rayburn House Office Building
Washington, D.C.

Chairman William Hurd, Chairman John Mica, and members of the House Subcommittees, thank you for the opportunity to testify today regarding the Internet of cars. My name is Khaliah Barnes, and I am the Associate Director and Administrative Law Counsel of the Electronic Privacy Information Center ("EPIC"). EPIC is an independent, non-profit research organization focused on emerging privacy and human rights issues. We work closely with a distinguished advisory board, comprised of leading experts in law, technology, and public policy.[1] EPIC has worked extensively on the privacy and data security implications of the Internet of Things,[2] and the Internet of Cars in particular.[3]

EPIC has submitted comments in over forty federal agency rulemakings on a host of proposed privacy regulations, including the National Highway Traffic Safety Administration's ("NHTSA") 2012 proposal to mandate event data recorders ("EDRs") in vehicles manufactured after September 2014[4] and NHTSA's 2014 advanced notice of proposed rulemaking requiring vehicle-to-vehicle communications.[5] We have also commented extensively on the privacy implications of networked vehicles.[6]

---

[1] EPIC, *EPIC Advisory Board* (2015), https://epic.org/epic/advisory_board.html.
[2] *E.g.*, EPIC, *Internet of Things (IoT)* (2015), https://epic.org/privacy/internet/iot/; EPIC, Comments on the Privacy and Security Implications of the Internet of Things, Fed. Trade Comm'n (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.
[3] *E.g.*, EPIC, Comments on the Federal Motor Vehicle Safety Standards: "Vehicle-to-Vehicle (V2V) Communications", Nat'l Highway Traffic Safety Admin., Docket No. NHTSA-2014-0022 (Oct. 20, 2014), https://epic.org/privacy/edrs/EPIC-NHTSA-V2V-Cmts.pdf; EPIC et al., Comments on the Federal Motor Vehicle Safety Standards; Event Data Recorders, Nat'l Highway Traffic Safety Admin., Docket No. NHTSA-2012-0177 (Feb. 11, 2013), https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf; *see generally* EPIC, *State Auto Black Boxes Policy* (2015), https://epic.org/state-policy/edr/; EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy* (2015), https://epic.org/privacy/edrs/.
[4] EPIC et al., Comments on the Federal Motor Vehicle Safety Standards; Event Data Recorders, *supra* note 3.
[5] EPIC, Comments on the Federal Motor Vehicle Safety Standards: "Vehicle-to-Vehicle (V2V) Communications", *supra* note 3.
[6] *See, e.g.*, Marc Rotenberg, *Are 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.

Summary

New vehicle technologies offer a variety of new services to American drivers, and are being quickly implemented by car manufacturers. But these new technologies also raise serious safety and privacy concerns that Congress needs to swiftly address. Current approaches, based on industry self-regulation, are inadequate and fail to protect driver privacy and safety. Increased congressional engagement and oversight of the Internet of Cars is imperative, as this fast-evolving industry affects the safety and privacy of millions of Americans on a daily basis. Specifically, Congress should act on pending legislation and grant NHTSA rulemaking authority over the Internet of Cars. NHTSA in turn should issue privacy rules that protect driver data and cybersecurity rules that prohibit malicious hacking of connected cars.

It is important that Congress is engaged on this critical issue. As described below, the Internet of Cars presents substantial privacy and security risks that warrant meaningful privacy and cybersecurity safeguards.

I. The Internet of Cars Presents Substantial Privacy and Security Risks

The Internet of Things ("IoT") is an ever-expanding network capable of connecting to devices and people through the Internet and other communications technologies.[7] Cars make up a significant segment of the IoT, with new vehicle technologies offering consumer services such as on-board navigation and tire pressure monitoring. But they also raise substantial safety and privacy concerns that Congress needs to address through meaningful privacy and cybersecurity safeguards.

Modern cars contain dozens of small computers, known as electronic control units, which are linked together by the car's internal computer network.[8] These

---

[7] EPIC, *Internet of Things (IoT)* (2015), https://epic.org/privacy/internet/iot/.

[8] *See Tracking & Hacking: Security & Privacy Gaps Out American Drivers at Risk*, Sen. Edward J. Markey (D-Mass.) (Feb. 2015) at 3–4, http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [hereinafter "Markey Report"]; David Gelles, Hiroko Tabuchi & Matthew Dolan, *Complex Car Software Becomes the Weak Spot Under the Hood*, N.Y. Times (Sept. 26, 2015), http://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html; Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/); Jim Motavalli, *The Dozens of Computers That Make Modern Cars Go (and Stop)*, N.Y. Times

computers control everything from braking, acceleration, steering, engine performance, door locks, and climate control to navigation and entertainment.[9] The system can also "record vehicle data to analyze and improve performance."[10]

A. Connected Cars Collect and Broadcast Troves of Sensitive Personal Data

As cars become more technologically sophisticated, they acquire the ability to collect and disclose huge amounts of sensitive driving data. According to one Senate report, about a third of all of cars from 13 major car manufacturers contain technologies that collect driving history information.[11] These technologies include "navigation, telematics, infotainment, emergency assist, stolen vehicle recovery, and event data recording systems."[12] Car manufacturers are able to collect volumes of personal information, including:

- Geographic/location information:
  - Physical location recorded at regular intervals;
  - Previous destinations entered into navigation system;
  - Last location parked.

(Feb. 4, 2010), http://www.nytimes.com/2010/02/05/technology/05electronics.html?_r=0. The electronic control units are referred to as "ECUs," and the internal computer network is operated by the control area network bus or "CAN" bus.

[9] *See* Gelles, Tabuchi & Dolan, *supra* note 8; Greenberg, *supra* note 8; Motavalli, *supra* note 8.

[10] Markey Report, *supra* note 8, at 3.

[11] *Id.* at 8.

[12] *Id.*

- Information generated by Event Data Recorders ("EDRs"):[13]
    - Potential crash events, such as sudden changes in speed;
    - Status of steering angle, brake application, seat belt use, and air bag deployment;
    - Fault or error codes in electronic systems.
- Operational information:
    - Vehicle speed;
    - Direction of travel;
    - Distances and times traveled;
    - Average fuel economy;
    - Status of power windows, doors, and locks;
    - Tire pressure;
    - Fuel level;
    - Tachometer reading (engine RPM gauge);
    - Odometer reading;
    - Mileage since last oil change;
    - Battery health;
    - Coolant temperature;
    - Engine status;
    - Exterior temperature and pressure.[14]

Internet-connected vehicles also have the ability to capture and store information around them. For example, the vehicles deployed by Google as part of the "StreetView" project captured not only digital imagery but also intercepted local WiFi communications, including "personal emails, usernames, passwords, videos, and

---

[13] EDRs are electronic "black boxes" that "record technical vehicle and occupant information for a brief period of time (seconds, not minutes) before, during and after a crash." Nat'l Highway Traffic Safety Admin., *Welcome to the NHTSA Event Data Recorder Research Web site*, http://www.nhtsa.gov/Research/Event+Data+Recorder+(EDR)/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site (last visited Nov. 13, 2015).

EDRs are now in the overwhelming majority of cars. Jim Motavalli, *Safety Agency Proposing Mandatory Event Data Recorders*, N.Y. Times Wheels Blog (Dec. 7, 2012), http://wheels.blogs.nytimes.com/2012/12/07/safety-agency-proposing-mandatory-event-data-recorders/ ("[A]pproximately 96 percent of model year 2013 cars and light-duty vehicles already have E.D.R. capability, the [National Highway Traffic Safety Administration] said.").

[14] Markey Report, *supra* note 8, at 8.

documents."[15] In other words, vehicles connected to the Internet were intercepting and storing private WiFi transmissions, obtained from residential networks. Google later discontinued this practice after it was discovered, though several court cases are still pending.[16]

The Google Streetview example is significant because it points to the likelihood that in the rapidly evolving world of connected cars, many vehicles may have sensory capabilities hidden from the view of operators, and much of the data generated by vehicles may be stored by remote computing services.[17] Last year, Google announced the "Open Automotive Alliance (OAA)," a global alliance of technology and auto industry companies committed to bringing the Android platform to cars.[18] The OAA includes Audi, GM, Google, Honda, Hyundai and Nvidia.[19] Congress should consider this issue as well as it explores the long-term significance of Internet-enabled vehicles.

---

[15] *Joffe v. Google, Inc.*, 746 F.3d 920, 923 (9th Cir. 2013); *see* EPIC, *Investigations of Google Street View* (2015), https://epic.org/privacy/streetview/; EPIC, *Ben Joffe v. Google* (2015), https://epic.org/amicus/google-street-view/; David Streitfeld, *Google Concedes That Drive-By Prying Violated Privacy*, N.Y. Times (Mar. 12, 2013), http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?pagewanted=all&_r=0.

[16] *See, e.g.*, In re: *Google Inc. Street View Electronic Communications Litigation*, No. 3:2010-md-02184 (N.D. Cal.); Sarah Gray, *Google must now face lawsuit over Street View privacy invasion*, Salon (June 30, 2014), http://www.salon.com/2014/06/30/google_must_now_face_lawsuit_over_street_view_privacy_invasion/.

[17] *See* Matt Swider, *Android Auto: the ultimate guide to Google navigation in the car,* TechRader (June 9, 2015), http://www.techradar.com/us/news/phone-and-communications/mobile-phones/android-auto-the-ultimate-guide-to-google-navigation-in-the-car-1277409

[18] Open Automotive Alliance, http://www.openautoalliance.net (last visited Nov. 17, 2015).

[19] *Press Room*, Open Automotive Alliance, http://www.openautoalliance.net/#press (last visited Nov. 17, 2015).

Car Manufacturers' Current Practices Provide Consumers Only With Notice of Data Collection

The majority of car manufacturers only inform consumers of data collection practices in owner's manuals, privacy policies, or terms and conditions, which are often long and largely unread.[20] These notices fail to inform consumers about the true scope of data being collected, and few give consumers true control over their data. Although some manufacturers allow consumers to delete already recorded data, preventing the car from constantly collecting and transmitting new data will often require "disabling valuable vehicle features or services."[21]

For example, the "Vehicle Data Recording and Privacy" section in the owner's manual of the General Motors 2016 Chevrolet Colorado vaguely notes that various systems in the truck will "store data" about engine and transmission performance conditions for airbag deployment, antilock braking, and "how the vehicle is operated, such as rate of fuel consumption or average speed."[22] The owner's manual also vaguely warns of data collection by the car's OnStar system and its navigations system, but requires drivers to track down separate policies to learn more about the data collected by these technologies.[23]

The MyLink Infotainment System Guide for the 2016 Chevrolet Colorado fails to clarify what incidental personal information may be collected.[24] To its credit, however, the manual explains how users can clear all private data, such as phone history or recent destinations.[25] The infotainment manual also includes, however, licenses from third-party software providers that may collect additional information.[26]

The Tesla Model S owner's manual states in vague terms that the computers throughout the vehicle "monitor and record data from various vehicle

---

[20] *Id.* at 12.
[21] *Id.* at 11.
[22] *Colorado*, Chevrolet, 372, https://my.chevrolet.com/content/dam/gmownercenter/gmna/dynamic/manuals/2016/Chevrolet/Colorado/2k16colorado1stPrint.pdf [hereinafter "Chevrolet Owner's Manuel"].
[23] *Id.* at 374.
[24] *Id.*
[25] *Chevrolet MyLink Infotainment System*, Chevrolet, 97 (2016), https://my.chevrolet.com/content/dam/gmownercenter/gmna/dynamic/manuals/2016/Chevrolet/Multi-Model%20PDFs/2k16chevroletmylink2ndPrint.pdf.
[26] *Id.* at 102 (Gracenote license).

systems," including the driving and vehicle conditions; motor, battery, braking and electrical system; speed, direction, and location.[27] Not only does Tesla—*not* the driver—control the collection and retention of driver data, the company also affirmatively refuses to give the driver copies of her data, even upon request.[28]

The owner's manual for the 2016 Toyota Camry explains that the car "is equipped with several sophisticated computers that will record certain data," such as engine speed, accelerator status, brake status, vehicle speed, and shift position.[29] The manual does clarify that the car does not record "conversations, sounds, or pictures."[30] The manual does not, however, give the driver control over the collection and retention of driving information.

Car Manufacturers Store Personal Driving Information Onboard the Car and at External Locations With Limited Security.

Some manufacturers only store personal driver information onboard the car.[31] However, a majority of car manufacturers transmit personal driver information from the car to external locations for storage.[32] For example, Tesla states in the owner's manual for the Model S that driving information "is stored by the vehicle and may be accessed, used and stored by Tesla service technicians during vehicle servicing or periodically transmitted to Tesla wirelessly through the vehicle's telematics system."[33] Many companies contract with third parties to provide data collection and storage services.[34] Moreover, the majority of manufacturers who collect driver data disclose it to third parties for unknown purposes.[35]

---

[27] *Model S Owner's Manual*, Tesla, 155, https://www.teslamotors.com/sites/default/files/Model-S-Owners-Manual.pdf (last visited Nov. 14, 2015) [hereinafter "Tesla Owner's Manual"].
[28] *Id.* ("Tesla does not disclose the data recorded to an owner unless it pertains to a non-warranty repair service and in this case, will disclose only the data that is related to the repair.").
[29] *2016 Toyota Camry - Owner's Manual*, Car Manuals 9 (2015) https://carmanuals2.com/get/toyota-camry-2016-owner-s-manual-72641 [hereinafter "Toyota Owner's Manual"].
[30] *Id.*
[31] Markey Report, *supra* note 8, at 10.
[32] *Id.*
[33] Tesla Owner's Manual, *supra* note 27, at 155.
[34] Markey Report, *supra* note 8, at 10.
[35] *Id.* at 11.

Alarmingly, it appears that few, if any, cars that store personal driver information onboard the vehicle use security systems to prevent remote access to the data.[36] Some manufacturers appear ignorant of the ability of remote hackers to use wireless ports to access the data (see section I.C).[37] There also appear to be few protections for personal driver data while it is wirelessly transmitted to other locations, and even less attention paid to stripping externally stored driver data of personally identifiable information.[38]

Car Manufacturers Use and Disclose Personal Driving Information for Vaguely Defined Purposes

In addition, car manufacturers use personal driving information for various but vague purposes, which leaves consumers in the dark about who has access to their information and why.[39] Personal driving information is often retained for years, if not indefinitely.[40]

For example, the owner's manual for the Chevrolet Colorado explains that the truck is equipped with an EDR.[41] General Motors promises not to access or disclose data generated by the EDR except "with the consent of the vehicle owner or, if the vehicle is leased, with the consent of the lessee; in response to an official request by police or similar government office; as part of GM's defense of litigation through the discovery process; or as required by law."[42] Data received by General Motors "may also be used for GM research needs or may be made available to others for research purposes, where a need is shown and the data is not tied to a specific vehicle or vehicle owner."[43]

The manual for the Toyota Camry states, "Toyota may use the data recorded in these computers to diagnose malfunctions, conduct research and development, and improve quality."[44] In addition, Toyota will disclose the data to third parties with the driver's consent, in response to an official request by police or a court, for use by Toyota in a lawsuit, and "[f]or research purposes where the data is not tied to a specific vehicle

---

36 *Id.*
37 *Id.*
38 *Id.*
39 *Id.*
40 *Id.*
41 Chevrolet Owner's Manual, *supra* note 22, at 373.
42 *Id.*
43 *Id.*
44 Toyota Owner's Manual, *supra* note 29, at 9.

or vehicle owner."[45] Toyota will also use data recorded by the 2016 Camry's EDR "for research on vehicle safety performance" and may "[d]isclose the data to a third party for research purposes without disclosing information about the specific vehicle or vehicle owner."[46]

Tesla states that it uses the data collected for various purposes, including "providing [the driver] with Tesla telematics services; troubleshooting; evaluation of [the] vehicle's quality, functionality and performance; analysis and research by Tesla and its partners for the improvement and design of [Tesla] vehicles and systems; and as otherwise may be required by law."[47] Tesla will also disclose driver data with third parties "for research purposes without disclosing details of the vehicle owner or identification information" and with "Tesla affiliated compan[ies], including their successors or assigns, or our information systems and data management providers."[48]

Notably, despite giving itself and its partners relatively free rein to access and use drivers' data, Tesla will not disclose the driver's data to the driver herself: "Tesla does not disclose the data recorded to an owner unless it pertains to a non-warranty repair service and in this case, will disclose only the data that is related to the repair."[49]

Third-party Telematics Systems Pose Additional Privacy Risks

Many modern cars contain "telematics" systems, which "use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider."[50] OnStar, a subscription telematics service, collects a wealth of personal information, including:

- Account information: name, address, telephone number, email address, license place number, emergency contact information, billing information, vehicle acquisition information such as date of purchase, information about how the driver uses the vehicle's features and systems, the driver's online activities over

---

[45] *Id.*
[46] *Id.* at 10.
[47] Tesla Owner's Manual, *supra* note 27, at 155.
[48] *Id.*
[49] *Id.*
[50] 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) [hereinafter "GAO Location Data Report"].

time and across different websites, IP addresses, device types, browser versions, pages viewed, searches made, customer proprietary network information;
- Vehicle information: the vehicle's identification number, make, model, year, diagnostic data, odometer readings, oil life remaining, tire pressure, fuel economy, refueling or recharging information, glass breakage, ignition switch activity, collision information;
- Driving information: the location of vehicle, GPS speed of vehicle, safety belt usage.[51]

According to 2014 Government Accountability Office testimony, the collection and sharing of consumer location information by in-car navigation providers poses serious risks to consumer privacy.[52] Storing location information over time "create[s] a detailed profile of individual behavior, including habits, preferences, and routes traveled," the exploitation of which can lead to identity theft or threats to personal safety.[53] In particular, the GAO report noted that in-car navigation providers "use different de-identification methods that may lead to varying levels of protection for consumers."[54]

According to its privacy policy, OnStar uses personal account, vehicle, and driving information for a variety of uses, including "[t]o provide you with offers for products or services that may interest you, including online offers based on your previous online activities and, with your prior additional consent, offers based on the location of your vehicle," "[f]or troubleshooting, evaluation of use, and research," "[t]o improve our products and Services," and "[t]o protect the safety of you or others."[55] OnStar will disclose driving information to General Motors "for product safety or security purposes, to protect the safety of you or others, or to help maintain the proper operation of your vehicle" (among other purposes).[56] It also discloses account and vehicle information with unnamed third parties "for marketing purposes."[57]

---

[51] *OnStar Privacy Policy*, OnStar (June 1, 2014), https://www2.onstar.com/web/portal/privacy?g=1.
[52] GAO Location Data Report, *supra* note 50, at 2.
[53] *Id.*
[54] *Id.*
[55] *OnStar Privacy Policy*, *supra* note 51.
[56] *Id.*
[57] *Id.*

B. Third Parties Can Access and Use Sensitive Driver and Driving Data

Data generated by new automobile technologies have a significant potential for secondary uses. For example, the owner's manuals and privacy policies from General Motors, Toyota, Tesla, and OnStar all stated that they would disclose information to law enforcement or as required by law.[58] Where car manufacturers and service providers are collecting and retaining information simply because they can, the ability of law enforcement to access this data risks could create entirely new and highly attractive methods of domestic surveillance.

The ability of connected cars to generate, store, and transmit sensitive driving information has also let to the development of "Usage-Based Insurance" ("UBI").[59] UBI allows automobile insurance to set premiums based on a driver's mileage and driving behavior.[60] Insurance companies collect data "using odometer readings or in-vehicle telecommunication devices (telematics) that are usually self-installed into a special vehicle port or already integrated in original equipment installed by car manufactures."[61] The driving data they collect includes "miles driven; time of day; where the vehicle is driven (GPS); rapid acceleration; hard breaking; hard cornering; and air bag deployment."[62]

Although UBI currently accounts for just two percent of U.S. personal car insurance policies,[63] the market for sensitive driving information is growing: "36 percent of all auto insurance carriers are expected to use telematics UBI by 2020."[64] For example,

---

[58] *See, e.g.*, Tesla Owner's Manual, *supra* note 27, at 155 (explaining that driver information will be shared disclosed when "[o]fficially requested by the police or other authorities"); Toyota Owner's Manual, *supra* note 29, at 9 (stating that driver information will be shared disclosed "[i]n response to an official request by the police, a court of law or a government agency"); Chevrolet Owner's Manual, *supra* note 22, at 373 (stating that EDR data will be shared disclosed "in response to an official request by police or similar government office"); *OnStar Privacy Policy*, *supra* note 51.

[59] *Usage-Based Insurance & Telematics*, Nat'l Ass'n of Ins. Comm'rs (Oct. 8, 2015), http://www.naic.org/cipr_topics/topic_usage_based_insurance.htm.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *2014 Usage-Based Insurance (UBI) Research Results for Consumer and Small Fleet Markets*, LexisNexis 3 (Aug. 2014), http://www.lexisnexis.com/risk/downloads/whitepaper/2014-ubi-research.pdf.

[64] *Usage-Based Insurance & Telematics*, *supra* note 59.

UBI programs such as State Farm's Drive Safe & Save[65] and Progressive's Snapshot[66] collect the miles driven, acceleration, braking, right and left turns, speeds over 80 mph, and the time of day the vehicle is driven, and use the data to calculate insurance rates.[67] The data is collected through telematics service providers such as OnStar and SYNC,[68] or through the installation of a data collection device into the car's diagnostic port such as In-Drive.[69]

The actuarial interest in detailed driving information will only grow, particularly as the Internet of Cars facilitates more granulated data collection. UBI should never be a mandatory component of auto insurance, and insurers should be barred from using driving information to calculate insurance premiums without the driver's consent. Auto insurers must not disclose or sell drivers' sensitive information to third parties. They should also be required to minimize the collection and storage of personally identifiable information, and to delete information as soon as insurers no longer need it to calculate insurance premiums.

Drivers also risk having their sensitive driving and vehicle data disclosed or sold to unknown third parties for marketing purposes. For example, OnStar discloses account and vehicle information to nameless third parties with which OnStar contracts "for joint marketing initiatives."[70]

---

[65] *Drive Safe & Save,* State Farm, http://www.statefarm.com/insurance/auto_insurance/drive-safe-save/drive-safesave.asp (last visited Nov. 14, 2015).
[66] *Snapshot: How Snapshot Works*, Progressive, http://www.progressive.com/auto/snapshot-how-it-works.aspx (last visited Nov. 14, 2015).
[67] *See, e.g.*, *Drive Safe & Save™ with In-Drive*, State Farm https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive (last visited Nov. 15, 2015); *Snapshot Privacy Statement*, Progressive (Nov. 18, 2014) https://www.progressive.com/auto/snapshot-privacy-statement/.
[68] *Drive Safe & Save with SYNC*, State Farm, https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/sync (last visited Nov. 14, 2015).
[69] *How It Works – Overview*, In-Drive, http://www.in-drive.com/sf/howItWorks.html#IL (last visited Nov. 14, 2015).
[70] *OnStar Privacy Policy*, *supra* note 51.

C. The Lack of Data Security Within the Internet of Cars Places Drivers at Risk of Physical Injury and Privacy Harms

Nearly all cars on the road today include at least one wireless entry point ("WEP").[71] WEPs are essential to the functionality of built-in wireless features such as tire pressure monitoring systems, "Bluetooth, keyless entry, remote start, navigation, Wi-Fi, cellular/telematics, radio, and anti-theft systems and features."[72]

Unfortunately, WEPs also provide entry points for remote vehicle hacking. A 2011 report by computer scientists showed how a hacker could use WEPs to "take control of various features — like the car locks and brakes — as well as to track the vehicle's location, eavesdrop on its cabin and steal vehicle data."[73]

In a 2013 study, researchers Charlie Miller and Chris Valasek connected laptops to the computer systems of a Toyota Prius and a Ford Escape and were able to jerk the wheel at high speeds, turn the car, cause sudden acceleration or braking, turn on the horn, tighten the seatbelts in anticipation of a nonexistent crash, and kill the brakes.[74] In 2014, a researcher wirelessly killed a car's engine and disabled its brakes as it drove up a ramp.[75] Earlier this year, Miller and Valasek wirelessly hacked a Jeep Cherokee traveling on a highway ten miles from their computers.[76] The pair were able to manipulate the air conditioning, turn on the radio, activate the windshield wipers and wiper fluid, take over the car's digital display screen, cut the transmission, kill the engine, and engage and

---

[71] Markey Report, *supra* note 8, at 5.
[72] *Id.*
[73] John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. Times (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html.
[74] 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; 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-Cars-Open-New-Doors-To-Smarter-Thieves.
[75] Xavier Aaronson, *We Drove a Car While It Was Being Hacked*, Motherboard (May 29, 2014), http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked.
[76] Greenberg, *supra* note 8.

disable the brakes.[77] In response to the reported hack, Fiat Chrysler recalled more than 1.4 million vehicles.[78]

So far, researchers and scientists in controlled settings have done most of the reported hacks of moving cars.[79] But wide scale malicious automobile hacking is certainly imminent, if not already occurring. Thieves can already hack computer-based door lock systems to rob parked cars.[80] And in 2010, a disgruntled former car salesman disabled more than 100 cars in Austin, Texas by hacking into a "web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments."[81]

The very real possibility of remote car hacking poses substantial risks to driver safety and security. Cars can be remotely hacked and controlled from anywhere in the world via the Internet.[82] Wireless hacking can also give hackers access to the car's physical location using built-in GPS navigation systems, which would facilitate crimes such as harassment, stalking, and car theft.[83]

Hackers can also gain access to the wealth of personal driver information accumulated by the car's computers. As noted by the Federal Trade Commission ("FTC"), identity theft is the number one complaint among American consumers.[84] According to the most recent Department of Justice study, more than sixteen million Americans were the victims of identity theft in 2012 alone, which cost more than twenty-

---

[77] *Id.*
[78] Alex Hern, *Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking*, The Guardian (Sept. 7, 2015), http://www.theguardian.com/technology/2015/sep/07/fiat-chrysler-recalls-more-jeeps-wireless-hacking; Reem Nasr, *Fiat Chrysler recalling 1.4M vehicles amid hacking defense*, CNBC (July 24, 2015), http://www.cnbc.com/2015/07/24/fiat-chrysler-recalling-14m-vehicles-amid-hacking-defense.html.
[79] *See, e.g.*, *id.*; Aaronson, *supra* note 75; Markoff, *supra* note 73; Miller & Valasek, *supra* note 74.
[80] Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. Times (Apr. 15, 2015), http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html?_r=0.
[81] Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, Wired (Mar. 17, 2010), http://www.wired.com/2010/03/hacker-bricks-cars/.
[82] Greenberg, *supra* note 8.
[83] *Id.*
[84] Fed. Trade Comm'n, Consumer Sentinel Network Data Book 3 (2015).

four billion dollars.[85] The Internet of Cars provides yet another means to gain access to sensitive and valuable consumer data.

Despite the real threat of remote WEP infiltration, "[m]ost automobile manufacturers were unaware of or unable to report on past hacking incidents."[86] Consumers have brought at least two nationwide class action lawsuits against car manufacturers for selling vehicles susceptible to hacking.[87]

II. Congress Must Enact Meaningful Safeguards for the Internet of Cars

A. The Auto Industry's Privacy Pledge Fails to Protect Driver Privacy

Every day without car privacy and safety protections places countless drivers at risk of having their personal information—or worse, their physical safety—compromised. Congress must act swiftly to combat the current and future privacy threats posed by the Internet of Cars.

Last year, a group of twenty automakers including General Motors and Toyota signed the Consumer Privacy Protection Principles for Vehicle Technologies and Services, a voluntary pledge in which the auto manufacturers stated their commitments to a set of privacy and data security principles.[88] While the pledge is an important first step for the industry to recognize consumer privacy issues and signal the significance to others in the market, the pledge is no substitution for federal baseline privacy protections.

---

[85] See Erika Harrell, Ph.D. & Lynn Langton, Ph.D., Bureau of Justice Statistics, Victims of Identity Theft 1, 6 (Dec. 12, 2013).

[86] Markey Report, *supra* note 8, at 5.

[87] *See, e.g.*, *Cahen et al. v. Toyota Motor Corp. et al*, No. 3:15-cv-01104 (N.D. Cal. filed Mar. 10, 2015) (suing Toyota, General Motors, and Ford on behalf of a nationwide class and bringing claims for class members in all fifty states); *Flynn et al v. FCA US LLC et al*, No. 3:15-cv-00855 (S.D. Ill. filed Aug. 4, 2015) (suing Chrysler to fix vulnerabilities in its uConnect infotainment system, as identified in a July 21, 2015 article by Wired Magazine: Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/).

[88] Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc., *Consumer Privacy Protection Principles for Vehicle Technologies and Services*, (Nov. 12, 2014) http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163.

First, the industry principles are "subject to change over time," and do not directly apply to the countless third-party service providers with whom auto manufacturers contract to collect driver information or other businesses with whom consumers directly engage to receive services.[89] Second, the pledge is premised on auto manufacturers providing drivers with notice and choice about the types of information the manufacturers collect, use, and disclose. Pledge participants may provide drivers notice in any way participants choose, including in "owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays."[90] But pledge members have broad authority to change the ways in which they collect, use, and disclose driver information and have wide discretion as to whether they should inform drivers of any changes in their privacy policies.[91]

Although pledge members commit to obtaining driver consent before using or disclosing driver location information, biometrics, and driver behavior information for marketing, the pledge grants members authority to use and disclose this sensitive driver personal information without consent for several broad purposes, including "for internal research or product development" or with third-party service providers providing "vehicle technologies and services."[92] The pledge even permits auto manufacturers to sell driver information pursuant to a company merger or acquisition.[93]

The constraints on the amount of data collected and how long auto manufacturers keep the information are unbounded: pledge participants can keep and store driver personal information as long as needed for "legitimate business purposes."[94] Although companies and their contractors collect a host of personal data, the pledge states that the members may provide drivers a way to correct and review only a limited subset of personal subscription information, like name, address, credit card numbers, telephone

---

[89] *Id*. at 2, 3–4.
[90] *Id*. at 6.
[91] Id. at 6–7 ("Notices need to be provided prior to every instances of collection where addressed by prior notices." "Participating Members commit to taking reasonable steps to alert Owners and Registered Users prior to changing the collection, use, or sharing practices associated with Covered Information in ways that have a material impact on Owners or Registered Users.").
[92] *Id*. at 8–9. "Vehicle technologies and services" is broadly defined as "technologies and services provided by, made available through, or offered on behalf of Participating Members that involve the collection, use, or sharing of information that is collected, generated, recorded, or stored by a vehicle." *Id.* at 5–6.
[93] *Id*. at 9.
[94] *Id.* at 11.

number or email address.[95] For other sensitive information like biometrics, members only commit to "exploring additional means" of providing drivers with "reasonable access" to their own driving information.[96]

Notwithstanding the various exceptions and loopholes the pledge provides, the pledge lacks any meaningful oversight and accountability mechanisms. In sum, the pledge supports the status quo of wholesale collection of sensitive driver personal information and fails to provide essential privacy protections.

B. Congress Should Act on Pending Legislation

There are several proposals currently before Congress that aim to put consumers back in the driver seat concerning personal privacy. The Security and Privacy in Your Car Act (SPY Car Act) of 2015,[97] would establish federal standards for connected cars.[98] The Act empowers NHTSA, in consultation with the FTC, to develop cybersecurity and privacy regulations for driver data collected by cars. The bill also calls for the creation of a "cyber dashboard" to inform consumers about how well each car protects privacy and security.

The Driver Privacy Act of 2015[99] would "establish limitations on data retrieval from vehicle" EDRs.[100] Because there are no current federal standards for the "ownership, use, or privacy of this data," the bill would "establish that the owner or lessee of a motor vehicle owns the data contained within the vehicle's EDR, and would create specific circumstances under which the data that is recorded or transmitted by an EDR can be accessed by entities other than the owner or lessee."[101]

---

[95] *Id*.
[96] *Id*.
[97] Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong.
[98] Press Release, Sen. Edward J. Markey, Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System (July 21, 2015), *available at* http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system.
[99] Driver Privacy Act of 2015, S. 766, 114th Cong.
[100] S. Rep. No. 114-147, at 1 (2015), *available at* https://www.congress.gov/114/crpt/srpt147/CRPT-114srpt147.pdf.
[101] *Id.*

And last month, the House Subcommittee on Commerce, Manufacturing, and Trade held a hearing[102] to consider a discussion draft on connected car privacy and security legislation. The House Subcommittee draft would require automobile manufacturers to develop modest privacy policies for the collection and use of driving and driver information.[103]

The draft falls short of providing robust privacy protections for drivers. First, the legislation would not require manufacturers to actually develop or implement any privacy protecting measures.[104] Instead, the privacy policies would only inform drivers about *whether* the manufacturer *chooses to* take various privacy-protecting measures. Moreover, a manufacturer who developed a privacy policy—regardless of whether it actually provided drivers with *any* privacy protections—would receive immunity from FTC scrutiny for unfair or deceptive business practices.[105] In other words, the weak privacy policy would block effective privacy safeguards.

The House draft would also require NHTSA to conduct a study on EDR data capture and retrieval.[106] Finally, the draft would impose civil penalties for vehicle hacking.[107]

EPIC broadly favors legislative proposals that safeguard the privacy of driver data. The most meaningful proposals incorporate the practices detailed in the Consumer Privacy Bill of Rights ("CPBR"). The CPBR is a sensible, comprehensive framework for privacy protection that provides substantive privacy protections, and would help establish fairness and accountability for the collection and use of driver personal information.[108] The CPBR enumerates seven fundamental consumer privacy principles that are central to the right of privacy and are found in many U.S. privacy laws: Individual Control,

---

[102] *Examining Ways to Improve Vehicle and Roadway Safety: Hearing on H.R. ___ before the Subcomm. on Commerce, Manufacturing, & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. (2015).

[103] _____ Act of 2015, H.R. ___, 114th Cong. § 301 (2015), *available at* http://docs.house.gov/meetings/IF/IF17/20151021/104070/BILLS-114pih-DiscussionDraftonVehicleandRoadwaySafety.pdf.

[104] *Id.* § 301(a) (§32402(b), "Vehicle Data Privacy – Identification Of Privacy Policy Requirements").

[105] *Id.* § 301(a) (§ 32402(e), "Vehicle Data Privacy – Safe Harbor").

[106] *Id.* § 301(b) ("Vehicle Data Privacy – Vehicle Event Data Recorder Study").

[107] *Id.* § 302.

[108] *See* Exec. Office of the President, Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012).

Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability.[109]

In the context of protecting the privacy of driver data, the Senate bills come much closer to safeguarding the interests of consumers than does the discussion draft currently in the House. In fact, we would oppose enactment of the House draft, which would be a step backward for Americans who are concerned about privacy and security.

In crafting cybersecurity legislation for connected cars, Congress should only issue civil fines for malicious hacking. This will encourage the necessary research to uncover security vulnerabilities, while at the same time discouraging hacking intended to cause harm.

The states, too, are moving in the right direction on car privacy. Seventeen states—Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington—have enacted statutes relating to event data recorders and privacy. Among other provisions, these states provide that data collected from a motor vehicle EDRs may only be downloaded with the consent of the vehicle owner or policyholder, with certain exceptions.[110] But more needs to be done.[111] There is an urgent need to establish meaningful and enforceable privacy and safety protections for the Internet of Cars. Self-regulatory industry codes of conduct, pledges, and multistakeholder processes routinely fail. Congress must move current proposals to protect driver data forward.

C. NHTSA Should Issue Driver Privacy Rules

The SPY Car Act of 2015, with its emphasis on enforceable NHTSA rules and civil fines for offenders, provides the type of privacy and security safeguards drivers need. Last month's House subcommittee on Commerce, Manufacturing, and Trade discussion draft on connected vehicle technology did not authorize a NHTSA privacy and security rulemaking and instead creates an "Automotive Cybersecurity Advisory

---

[109] *Id.* at 10.

[110] National Conference of State Legislatures, "Privacy of Data from Event Data Recorders," http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx

[111] *See generally* EPIC, *State Auto Black Boxes Policy* (2015), https://epic.org/state-policy/edr/.

Council" to establish cybersecurity best practices. But best practices will not provide the necessary privacy protections; enforceable rules will.

NHTSA plays a critical role in protecting driver information and data security. There are several privacy proposals currently before the agency. In 2012, the agency proposed to mandate EDRs in "most light vehicles manufactured on or after September 1, 2014."[112] NHTSA concedes that there are significant privacy concerns with the collection of this data: "The agency acknowledges that consumer privacy concerns persist regarding EDR data: Who owns it, who has access to it and under what circumstances, and what are the purposes for which it may be used."[113] The agency is also in the early stages of proposals to require vehicle-to-vehicle ("V2V") communications. NHTSA has acknowledged the consumer privacy issues arising with V2V technology, noting that these issues "are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA's decision about whether and, if so, how to proceed with V2V research or regulation."[114] The agency acknowledges that consumer privacy considerations are "inherent in mandated V2V technologies," and the agency has posed a number of questions regarding these privacy issues.[115]

As Congress moves forward, it is critical that NHTSA has rulemaking authority over this emerging industry. NHTSA should issue driver privacy rules based on the Consumer Privacy Bill of Rights. This framework would establish baseline safeguards for the development of innovative car technology while safeguarding individual privacy. But Congress must first enact baseline legislation with NHTSA rulemaking authority.

Lastly, meaningful implementation requires meaningful enforcement mechanisms. The SPY Car Act and the House's draft discussion legislation envision the FTC bringing Section 5 unfair and deceptive actions against auto manufacturers for misrepresentations regarding privacy and security. The FTC may have a role to play, but enforcement should not be assigned solely to the FTC. EPIC has studied the FTC's Section 5 enforcement for several years and has found that the FTC has failed to enforce

---

[112] Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571).
[113] *Id.* at 74,150.
[114] Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application, Nat'l Highway Traffic Safety Admin, 144 (Aug. 2014), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.
[115] *Id.*

its own orders when companies have breached settlement agreements.[116] The FTC infrequently undertakes enforcement actions. The FTC also lacks necessary competence to evaluate the specific privacy and security risks of connected vehicles.

It is clear that consumers desperately need stronger enforcement mechanisms than the FTC, including a private right of action against companies who misuse and fail to secure personal information. Private rights of actions are familiar remedies in U.S. privacy laws.[117]

Conclusion

The Internet of Cars raises substantial privacy and security concerns for American drivers and automobile manufacturers. One company has already recalled 1.4 million vehicles because of the risk of remote hacking. Almost twenty states have taken steps to regulate the collection and use of driver data.

It is time for Congress to act. EPIC recommends: (1) Congress enact meaningful legislation, based on enforceable legal rights, that safeguard the privacy and security of American drivers; (2) Congress establish civil fines for malicious hacking of vehicles; and (3) Congress grant NHTSA rulemaking authority to establish necessary safeguards for connected vehicles.

Congress should act quickly on these recommendations. There is a new danger to American drivers and the auto industry that can no longer be ignored.

Thank you for the opportunity to testify during today's hearing. I will be pleased to answer your questions.

---

[116] *See* Letter from EPIC to Rep. Darrell E. Issa, Chairman, Committee on Oversight & Government Reform, U.S. House of Representatives (July 25, 2015), *available at* https://epic.org/privacy/ftc/EPIC-Congress-re-FTC.pdf; *see also* EPIC, *EPIC v. FTC (Enforcement of the Google Consent Order)* (2015), https://epic.org/privacy/ftc/google/consent-order.html.

[117] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692–1692p; Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508; 100 Stat. 1848.