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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION &

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles

May 1, 2017

By notice published March 20, 2017 the Federal Trade Commission ("FTC") and the National Highway Traffic Safety Administration ("NHTSA") requested comments for upcoming workshop on the benefits, privacy, and security issues associated with current and future motor vehicles.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") hereby submits these comments and recommendations to address the privacy and security implications of connected vehicles.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights related issues, and to protect privacy, the First Amendment and constitutional values.[2] EPIC is a leading advocate for

[1] *FTC and NHTSA Seek Input on Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles,* FTC, Mar. 20, 2017, https://www.ftc.gov/system/files/attachments/press-releases/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues-related-connected-automated-vehicles/notice_connected_cars_workshop_with_nhtsa_1.pdf.

[2] *About EPIC,* EPIC, http://epic.org/epic/about.html.

consumer privacy and privacy enhancing techniques for emerging technology, such as connected cars and other devices compromising the "Internet of Things."[3] EPIC has considerable expertise in the Internet of Things and other connected devices and has testified before Congress on connected vehicles and submitted numerous comments to various agencies concerning connected devices.[4] Additionally, EPIC has submitted comments to NHTSA regarding the privacy risks inherent in Event Data Recorders and privacy considerations for automated vehicles.[5]

EPIC is pleased to see the FTC and NHTSA working jointly on the issue of connected vehicles. The development of connected vehicles has substantial implications for consumer protection, privacy, and safety. As both agencies determine what to discuss at the June workshop EPIC urges the agencies to include the following topics 1) data retention and storage 2) vehicle security 3) protecting consumer privacy and 4) the role of states in the development of connected vehicles.

I. Data Retention and Storage

Connected cars will have the ability to collect and store massive amounts of data on those who drive them, as well as collect personally identifiable information ("PII"). EPIC is

[3] *See*, *e.g.*, EPIC, *Consumer Privacy*, http://epic.org/privacy/consumer/; EPIC, *Big Data and the Future of Privacy,* https://www.epic.org/privacy/big-data/; EPIC, *Internet of Things (IoT),* http://epic.org/privacy/internet/iot/default.html.

[4] 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; EPIC Statement to the House Committee Subcommittee on Communications and technology, Feb. 2, 2017, https://epic.org/testimony/congress/EPIC-Statement-NTIA-02-02-2017.pdf; Comments to the NTIA "On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," June 2, 2016, https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

[5] Comments to NHTSA "Federal Motor Vehicle Safety Standards; Event Data Recorders," Feb. 11, 2013, https://epic.org/apa/comments/EPIC-Coalition-NHTSA-EDR-comments-FINAL-1.pdf; Comments to NHTSA "Request for Comment on 'Federal Automated Vehicles Policy,'" Nov. 22, 2016, https://epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf; Comments to NHTSA "Federal Motor Vehicle Safety Standards; V2V Communications," Apr. 12, 2017, https://epic.org/apa/comments/EPIC-NHTSA-V2V-Communications.pdf (hereafter "EPIV V2V Comments").

encouraged by the steps taken in NHTSA's recent vehicle-to-vehicle ("V2V") communications notice of proposed rulemaking ("NPRM") to minimize the amount of data collected and stored.[6] However, the Privacy Impact Assessment released concurrent with the NPRM discussed the possibility of a private, third-party entity that would be responsible for receiving and storing certain safety messages from vehicles.[7] The NPRM further went on to discuss the fact that the third-party entity would not necessarily be subject to federal record keeping or transparency laws.[8]

EPIC expects that various private entities will be involved in the development of connected vehicles. However, as these cars are developed data retention and storage should be a central concern to federal regulators and to private companies. The increase in the size and scope of data and security breaches in recent years cannot be understated.[9] As such, both agencies should urge all entities involved in the development of connected vehicles to limit the amount of data they collect and only store data that they need to keep. Failure to protect user privacy frequently stems from failure to adequately secure user data, which can result in enormous liability for companies.[10] The more data a company stores, the more valuable a target its database is for hackers; and the more stored data, the greater the company's losses in the event of a breach.[11]

---

[6] *Request for Comment on "Federal Motor Vehicle Safety Standards; V2V Communications,"* 82 Fed. Reg. 3854, 3904 (Jan. 12, 2017) (hereafter "V2V NPRM").
[7] *Privacy Impact Assessment: Notice of Proposed Rulemaking (NPRM) on V2V Communications,* Department of Transportation.
[8] *Id.* at 15.
[9] *See e.g.* John Kell, *Chipotle Says Its payment System Was Hacked,* Fortune, Apr. 25, 2017; Dan Goodin, *Call It a "Data Rupture": Hack Hitting OPM affects 21.5 Million,* Arts Technica, Jul. 5, 2015, Vindu Goel & Nicole Perloth, *Yahoo Says 1 Billion User Accounts Were Hacked*, New York Times, Dec. 14, 2016, https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.
[10] *2016 Cost of Data Breach Study: United States*, PONEMON INST., 1 (June 2016).
[11] Bruce Schneier, *Data Is A Toxic Asset*, SCHNEIER ON SECURITY, (March 4, 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html ("saving [data] is dangerous because failing to secure it is damaging. It will reduce a company's profits, reduce its market share, hurt

EPIC has long argued that the best way to prevent loss or misuse of sensitive personal information is to avoid gathering or storing it in the first place.[12] Data that is not collected or retained cannot be subject to unauthorized access or disclosure. Minimizing stored user data reduces incentives for hackers to attack data storage systems by reducing the amount of data available to steal. This practice also reduces the costs of data breaches.

Data protection is often discussed under the assumption that there is one primary owner of a device whose data is at risk of being compromised. However, with cars increasingly being able to connect to the internet, data security becomes a problem for virtually any driver of the car. The FTC recently noted that when an individual rents a car and connects their phone to that vehicle that the car can keep all of the data that they access for an indefinite period of time.[13] That is information that can be accessed by future renters, the rental car company, or any individual who hacks into a cars computer system. These are substantial concerns that must be

---

its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company's computers and networks.").

[12] *See, e.g.* Comments of EPIC, *Standards for Safeguarding Customer Information Request for Public Comment* (Nov. 7, 2016), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Rule-Comments-11-07-2016.pdf; Reply Comments of EPIC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 11-12, WC Docket NO. 16-106 (July 6, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf; Comments of EPIC, Request for Information: Big Data and the Future of Privacy (April 4, 2014), https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf; Brief of Amicus Curiae Electronic Privacy Information Center in Support of Respondent, *City of Ontario v. Quon*, 560 U.S. 746 (2010), https://epic.org/privacy/quon/Quon_Brief_Draft_final.pdf.

[13] 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.

[13] 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 ("Researchers have shown that it is both easy and cheap to surveil connected vehicles.").

addressed be quickly addressed as many consumers may currently be unaware that they have left substantial amounts of data in cars they have recently rented.

II. Vehicle Security and Safety

Connected cars have the possibility to present substantial safety and security risks. While companies continue to implement new technologies and test driverless cars, there is substantial evidence to show that those vehicles are incredibly vulnerable. In our previous comments to NHTSA we have detailed cases where researchers have been able to hack into vehicles and take control over them,[14] hacking into computer systems to unlock locked cars,[15] and how a disgruntled former car salesman was able to disabled more than 100 cars in Austin, Texas by hacking into a web based system.[16]

Recently, Charlie Miller, whose research led Chrysler to recall 1.4 million vehicles after he hacked into a Jeep,[17] left Uber for a position at Didi, a Chinese startup that is working on an autonomous ridesharing project. Miller recently stated that he left Uber partially because he wanted to speak more freely about the ability to hack cars and specifically noted the danger in self-driving ridesharing and taxi services.[18] Miller stated 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

---

[14] 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-remotelykill-jeep-highway/; Adam Greenberg, *The Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse*, Wired, Aug. 1, 2016, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration- hacks/.

[15] Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, New York Times (Apr. 15, 2015), http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[16] Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, Wired (Mar. 17, 2012), https://www.wired.com/2010/03/hacker-bricks-cars/.

[17] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 Million Vehicles For Bug Fix*, Wired, Jul. 24, 2015, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[18] 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/.

going to be even worse."[19] The potential risks that connected cars pose to the driver, as well as the potential risk to the public, cannot be understated.

Even where vehicles have not been tampered with, connected and autonomous vehicles pose several safety and security concerns. Google reported more than 200 failures in their autonomous vehicles that were being tested in California.[20] Uber recently suspended its self-driving car program after one of their autonomous vehicles was involved in an accident while going through a yellow light at an intersection.[21]

Of even greater concern are potential car systems that would require a driver to take control of a car with a moments notice. Distracted driving is already a problem on America's roadways[22] and the development of cars that can perform some driving functions but can still require an individual to take control of a car in some circumstances pose substantial problems. A Tesla owner was killed last year after driving his car in autopilot, a self-driving mode.[23] Perhaps what is most disturbing about this incident was the conclusion that the car performed as it should and that the driver was at fault for not paying attention.[24] The fact that the system operated as it was supposed to but that the driver did not have time to regain control of the vehicle demonstrates the problem with expecting driver to suddenly take control of their cars. There is likely no sufficient warning, either in the car or in a drivers manual, that would not lead a substantial number of consumers to believe that they need to stay alert while their car is

[19] *Id.*
[20] Mark Harris, *Google Reports Self-Driving Car Mistakes: 272 Failures and 13 Near Misses*, The Guardian, Jan. 12, 2016, https://www.theguardian.com/technology/2016/jan/12/google-self-driving-cars-mistakes-data-reports.
[21] Danielle Muoio, *Police: The Self-Driving Uber in the Arizona Crash Was Hit Crossing an Intersection on Yellow*, Business Insider, Mar. 30, 2017, http://www.businessinsider.com/uber-self-driving-car-accident-arizona-police-report-2017-3.
[22] *Study: Majority of Car Accidents Caused By Distracted Driving*, AOL, Apr. 4, 2017, https://www.aol.com/article/news/2017/04/04/study-majority-of-car-accidents-caused-by-distracted-driving/22024897/.
[23] Bill Vlasic & Neal E. Boudette, *Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says*, New York Times, Jun. 30, 2016.
[24] Neal E Boudette, *Tesla's Self-Driving System Cleared In Deadly Crash,* New York Times, Jan. 19, 2017, https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html.

supposed to be driving itself. This concern is what has led a number of automakers to skip this level of automation altogether.[25]

Security is not only an issue in connected cars, but throughout the entire Internet of Things ecosystem. A recent report by AT&T noted that there is a lack of guidelines or best practices for connected devices and that without those standards, many manufacturers do not incorporate sufficient security measures.[26] The report also notes that this lack of security becomes problematic when several companies work together to produce a connected product and that a security flaw in one can not only compromise the end product but can lead to confusion about who is ultimately responsible for the breach.[27] A connected car is the ultimate Internet of Things device. It has the potential to download data stored on your phone and makes it possible to determine where you work, live, worship, and can reveal several details about your personal life and habits. Sufficient security standards are needed for all Internet of Things devices, but they are especially necessary for vehicles.

III. Consumer Protection and Privacy

Consumer protection and privacy must be a consideration in the development of connected vehicles. While it appears as though substantial thought has been given to how connected cars should be developed, the role that consumers will play has not been as widely discussed. It is largely presumed that consumers want more technology in their cars and, eventually, a car with the ability to drive without any human controlling the driving process.

---

[25] James Ayre, *Ford: Skip Level 3 Autonomous Cars – Even Engineers Supervising Self-Driving Vehicle Testing Lose "Situational Awareness,"* Clean Technica, Feb. 20, 2017, https://cleantechnica.com/2017/02/20/ford-skip-level-3-autonomous-cars-even-engineers-supervising-self-driving-vehicle-testing-lose-situational-awareness/; Russ Mitchell, *When Robots and Humans Take Turns At The Wheel,* LA Times, Sep. 22, 2016, http://www.latimes.com/business/autos/la-fi-hy-driverless-levels-tesla-ford-gm-mercedes-volvo-google-20160922-snap-story.html; Alex Davies, *The Very Human Problem Blocking The Path To Self-Driving Cars*, Wired, Jan 1. 2017, https://www.wired.com/2017/01/human-problem-blocking-path-self-driving-cars/.

[26] *Blueprint for Cybersecurity Innovation*, AT&T, https://www.business.att.com/cybersecurity/cybersecurity-innovation/.

[27] *Id.*

Even if this is a correct assumption for the majority of consumers those desires should not be given into at the expense of consumers who do not wish to have such technology in their cars.

As connected cars are developed, consumers should always have the option to opt-out of using certain technology. As EPIC noted in our recent comments on V2V communications "Consumers should always have a choice about what technologies they do or do not use, especially if their privacy is at risk. Consumers should not be forced to use technology that poses a risk to their safety or security."[28]

In addition to data about the car itself, consumers should also be aware of how data tracking their location could be used. It is not unreasonable to conclude that some companies would seek to turn cars into an advertising mechanism. Targeted advertising is already employed by search engines and social media companies based on data collected by individuals who use them.[29] Connected vehicles pose the potential to be another mechanism to attempt to sell products to consumers based on where they travel.

What is needed to protect consumers in this emerging industry are meaningful oversight and enforcement mechanisms. Best practices and guidelines are voluntary practices and consumers have no recourse if these policies are violated. Leaving essential privacy and security protections to the discretion of carmakers and companies such as Google places consumers at risk.

For example, the recently issued Federal Automated Vehicles Policy states that any disclosure of data to third parties "should not contain any personally identifiable information."[30]

---

[28] EPIC V2V Comments at 6-7.
[29] Olivia Solon, *Google's Ad Tracking Is As Creepy As Facebook's. Here's How To Disable It,* The Guardian, Oct. 21, 2016, https://www.theguardian.com/technology/2016/oct/21/how-to-disable-google-ad-tracking-gmail-youtube-browser-history.
[30] Nat'l Highway Traffic Safety Admin., *Federal Automated Vehicles Policy,* Sep. 2016, https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016 (hereafter "Federal AV

However, consumers have no recourse if the Policy is violated. Similarly, the Policy states that cybersecurity practices "should be fully documented...and data should be traceable within a robust document version control environment."[31] However, the Policy itself provides no mechanism for enforcement.

Meaningful enforcement of privacy and security protections also requires 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 law and would be appropriate in the context of automated vehicles.[32]

IV. State involvement

EPIC is very concerned with indications from NHTSA that state law will be preempted in the development of connected and autonomous vehicles. The V2V communications NPRM would create a new Federal Motor Vehicle Safety Standard ("FMVSS") which would preempt states from going further in issuing their own regulations on connected cars.[33] Furthermore, the Federal Automated Vehicles Policy also envisions a limited role for states in the development of connected cars based on the traditional role that states and the federal government play in transportation.[34] However, connected cars are not traditional vehicles and a new approach is needed in their development that combines transportation, consumer protection, and privacy. Historically, federal privacy laws have not preempted stronger state law protections or

---

Policy").
[31] *Id.* at 21.
[32] *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.
[33] "When a motor vehicle safety standard is in effect under this chapter, a State or a political subdivision of a State may prescribe or continue in effect a standard applicable to the same aspect of performance of a motor vehicle or motor vehicle equipment only if the standard is identical to the standard prescribed under this chapter." 49 U.S.C. § 30102(b)(1).
[34] Federal AV Policy at 38.

enforcement mechanisms. In both the privacy and consumer protection context, federal regulations serve as baselines while allowing states to enact and enforce stronger laws.[35]

While the federal government has enacted privacy laws, more robust privacy legislation has been implemented at the state level. Many states have enacted privacy legislation that exists alongside federal law covering the same material. Furthermore, under *Hillsborough County v. Automated Medical Laboratories* there is currently a presumption that state and local governments are primarily responsible for matters related to health and safety.[36] Privacy is included in the area of health and safety regulations that are traditionally left to the states.[37]

It is clear that states have an interest in being involved in the development of connected vehicles. In 2016, 20 states introduced connected vehicle legislation.[38] In the first few months of 2017, 33 states have introduced connected vehicle legislation.[39] The industry as a whole would benefit from allowing states to play a role crafting regulations for connected cars as technology advances.

States have a unique perspective allowing them to develop innovative programs to protect consumers. Congressman David McKinley recently noted at a hearing on autonomous vehicles that his state of West Virginia has a landscape that presents unique challenges to connected vehicles such as tunnels and lack of access to strong wireless signals.[40] Problems such as this are precisely why states should be allowed to craft their own regulations in this process. State

---

[35] *See e.g.* Electronic Communications Privacy Act; Right to Financial Privacy Act; Cable Communications Privacy Act; Video Privacy Protection Act; Employee Polygraph Protection Act; Telephone Consumer Protection Act; Driver's Privacy Protection Act; Gramm-Leach-Bliley Act.
[36] *Hillsborough County v. Automated Medical Laboratories*, 471 U.S. 707 (1985).
[37] *See e.g. Hill v. Colorado*, 530 U.S. 703 (2000) (upholding a law that protected the privacy and autonomy of individuals seeking medical care because the law was intended to serve the traditional exercise of State police power to protect the health and safety of its citizens).
[38] *Autonomous Vehicles,* National Conference of State Legislatures, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.
[39] *Id.*
[40] *Self-Driving Cars: Levels of Automation,* U.S. House of Representative, Energy and Commerce Committee, Mar. 28, 2017, https://energycommerce.house.gov/hearings-and-votes/hearings/self-driving-cars-levels-automation.

legislatures are closer to their constituents and the entities that they regulate and are often the first to recognize trends and emerging problems, and are well suited to address new challenges and opportunities as they arise and as technology evolves.

Conclusion

EPIC looks forward to the FTC and NHTSA's upcoming workshop on connected vehicles. These vehicles pose many exciting opportunities but also present substantial challenges. We urge the agency to make data protection, vehicle safety, consumer protection, and privacy to be central topics at this workshop. We also urge the agencies to devote time to discussing the role that states could play in the development of this new technology.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow