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

DEPARTMENT OF TRANSPORTATION

Notice of Request for Comments: Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0)

Docket No. DOT–OST–2018–0149

December 8, 2018

By notice published October 9, 2018[1] the Department of Transportation ("DoT") requested public comment on a revised framework and multimodal approach to integrating automated driving technologies into the nation's transportation system, *Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0)*.[2] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to address the substantial privacy and security implications of automated 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 issues, and to protect civil liberties, the First Amendment, and constitutional values.[3] EPIC is a leading advocate for privacy and privacy-enhancing techniques for emerging technology, such as connected cars and automated devices

[1] *Notice of Request for Comments: Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0)*, 83 Fed. Reg. 50746 (Oct. 9, 2018).
[2] *Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0),* DoT, https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf (hereafter, "Proposed Framework").
[3] *About EPIC*, EPIC, https://epic.org/epic/about.html.

comprising the "Internet of Things."[4] EPIC has considerable experience in the Internet of Things and connected vehicles. EPIC testified before Congress and submitted comments to various agencies, including the Federal Trade Commission and the National Highway Traffic Safety Administration ("NHTSA"), concerning the privacy and safety risks of automated vehicles.[5]

EPIC supports federal regulations to guide the development and deployment of automated vehicles in the United States. The development of automated vehicles raises many issues for consumer protection, privacy, and public safety. EPIC urges DoT to revise the Proposed Framework to (1) highlight certain safety and security risks caused by automated vehicles; (2) underscore the importance of safeguarding consumers' right to privacy when developing automated vehicles; (3) promulgate obligatory rather than voluntary industry guidance to increase consumer protection; and (4) emphasize the need for government involvement in establishing cybersecurity best practices for automated vehicles.

I. Automated vehicles pose significant safety risks

Automated vehicles present numerous safety and security risks that can lead to serious physical harm. While companies continue to implement and test automated driving technologies,

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

[5] *See, e.g.,* EPIC Comments to the FTC and NHTSA, "Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles," May 1, 2017, https://epic.org/apa/comments/EPIC-ConnectedCar-Workshop-Comments.pdf; 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; EPIC 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. EPIC 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; EPIC 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; EPIC 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").

there is substantial evidence illustrating the vulnerability of automated vehicles. In previous comments to the FTC and NHTSA EPIC has illustrated some of these security vulnerabilities, including instances where researchers have unlocked locked cars[6] and taken control[7] of moving vehicles by hacking computer systems. Although DoT included cybersecurity breaches in a list of potential safety concerns related to automated vehicles, the Proposed Framework does not make clear that cybersecurity breaches can directly cause physical harm to the driver and to surrounding individuals.[8]

Security vulnerabilities increase risks of theft and other malicious activities. Six years ago a disgruntled former car salesman disabled over 100 vehicles in Austin, Texas by hacking into a connected network.[9] Since then, hacking has gotten much worse. Car dealers have activated kill switches to shut down cars remotely while vehicles are in motion if customers are late on car payments, leaving drivers physically stranded and/or placing them and surrounding vehicles in grave danger on roads and highways.[10] Researchers have also demonstrated how automated vehicles can be wirelessly hacked over the Internet from anywhere in the world,[11] giving thieves access to a car's physical location to enable car theft. Given that stalkers and domestic abusers have also exploited

[6] 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.
[7] 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/.
[8] Proposed Framework at 13.
[9] Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, Wired (Mar. 17, 2012), https://www.wired.com/2010/03/hacker-bricks-cars/.
[10] Elaine S. Povich, *Late Payment? A 'kill switch' Can Strand You and Your Car*, Pew Research (Nov. 27, 2018), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/11/27/late-payment-a-kill-switch-can-strand-you-and-your-car.
[11] *Hackers Remotely Kill a Jeep on the Highway – With Me in It*.

geolocation data to track victims' location and record victims' calls,[12] the data security risks of connected cars constitute serious public safety concerns.[13]

Security vulnerabilities of autonomous vehicles could also devastating effects on drivers, passengers, those in other vehicles, and pedestrians. As early as 2013, researchers Charlie Miller and Chris Valasek manipulated the control systems of a Toyota Prius and a Ford Escape after connecting the automated vehicles to a laptop, from which they could cause sudden acceleration, sound the car horn, and disable the brake system while the cars were in motion.[14] 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 going to be even worse."[15] Chrysler later recalled 1.4 million vehicles after similar vulnerabilities were discovered that allowed hackers to activate the car's windshield wipers and wiper fluid, cut transmission, kill the engine, and cause sudden braking.[16] In 2017, security researchers in China were able to hack a Tesla Model X so that they could turn on the brakes and unlock the car's doors remotely.[17]

The potential risks that automated vehicles pose to the driver and the public cannot be overstated. EPIC urges the agency to revise the Proposed Framework to make clear the risks to public safety that could result from deploying automated vehicles in the United States.

---

[12] William Turton, *Abusive Partners Are Now Tracking Their Spouses With Apps Made to Watch Their Kids*, Vice News (Sept. 16, 2018), https://news.vice.com/en_us/article/ev7n44/abusive-partners-are-now-tracking-their-spouses-with-apps-made-to-watch-their-kids.

[13] *Hackers Remotely Kill a Jeep on the Highway – With Me in It.*. *See also* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, Motherboard (Ju. 25, 2016), https://motherboard.vice.com/en_us/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

[14] *Hackers Remotely Kill a Jeep on the Highway – With Me in It.*

[15] *Id*.

[16] *Id.*

[17] Ellen Daniel, *What Can Be Done to Stop Connected Car Hacking?* Verdict (Jun. 26, 2018), https://www.verdict.co.uk/connected-car-hacking-driverless-cars/.

II. DoT should prioritize consumers' right to privacy to "protect and enhance freedoms enjoyed by Americans"

One of the six principles in the Proposed Framework is a commitment to "protect and enhance the freedoms enjoyed by Americans."[18] The DoT stated that the proliferation of automated vehicles supports this objective by increasing consumer mobility choices to meet the needs of older Americans and those with disabilities.[19] However, the principle does not mention the need to safeguard Americans' right to privacy, a freedom that is put at risk by automated driving systems.

Without privacy standards regulating access to vehicle data, the freedom of Americans will be diminished.[20] For example, Uber—one of the leading companies developing autonomous vehicles—has a history of abusing the location data of its customers. Individual employees could use "God View," an "easily accessible" internal company tool to obtain a specific user's real-time and historic location and track a user in real time.[21] The federal government[22] and many states have also enacted privacy laws to limit access to vehicle data by the police, insurance companies, and others.[23]

These risks are clear. A Ford executive said in 2014 that vehicle tracking data was being used for law enforcement purposes: "We know everyone who breaks the law, we know when you're

---

[18] Proposed Framework at v.
[19] *Id*.
[20] *See* Marc Rotenberg and Natasha Babazadeh, *U.S. Supreme Court Affirms Fourth Amendment in Rental Car Search, Steers Clear of Commercial Contract Limitation (Byrd v United States)*, 4 European Data Protection L. Rev. 400 (September 26, 2018), https://edpl.lexxion.eu/article/EDPL/2018/3/23; *see also* Brief of EPIC as Amicus Curiae in Support of Petitioner, *Byrd v. United States*, 584 U.S. __, https://epic.org/amicus/fourth-amendment/byrd/Byrd-v-US-EPIC-Amicus-Brief.pdf.
[21] Johana Bhuiyan & Charlie Warzel, *"God View": Uber Investigates Its Top New York Executive For Privacy* Violations, Buzzfeed (Nov. 18, 2014), http://www.buzzfeed.com/johanabhuiyan/uber-is- investigating-its-top-new-york-executive-for-privacy#.scM0ymqne; *see also Complaint of EPIC to the FTC against Uber*, Jun. 22, 2015, https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.
[22] Driver's Privacy Protection Act, Pub. L. 103-322 (1994).
[23] *See, e.g.,* Arkansas Code § 23-112-107 (requiring disclosure of event data recorders in vehicles by written notice at time of purchase, and in writing with subscription services); Delaware Code § 3918 (prohibits insurance companies from downloading recorder data without consent of the policy holder). *See also* Privacy of Data From Event Data Recorders: State Statutes, National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

doing it. We have GPS in your car, so we know what you're doing."[24] Although the U.S. Supreme Court recently held that mobile geolocation data is protected from unreasonable search and seizure under the Fourth Amendment,[25] this ruling does not prevent user data from automated cars from being misused in other ways, such as those which cause harassment. For example, top Uber executives used the same God View technology to track journalists who wrote critical stories about the company.[26] In order for DoT to achieve its mission to protect and enhance American freedoms, EPIC urges the agency to establish clear privacy safeguards to govern the collection and use of personal data. These standards should apply Fair Information Practices[27] – an internationally recognized set of informational privacy practices – in order to provide comprehensive privacy protections for autonomous vehicles.

III. Voluntary guidance is insufficient to protect consumers

The Proposed Framework provides voluntary, rather than mandatory, multimodal safety guidance, which is insufficient to provide meaningful consumer protection. At best, the Proposed Framework gives automotive vehicle developers and manufacturers a range of initiatives that *should* be done, but not which *must* be done. For example, the Proposed Framework encourages but does not require automated driving system developers to make Voluntary Self-Assessments public to increase transparency and public confidence in the technology.[28] Developers not only have the option to avoid making safety assessments of their products, but they also have the choice to keep them secret if they do conduct them; neither outcome would promote transparency or public

[24] Eugene Volokh, "Ford 'Know[s] Everyone Who Breaks the Law' Using Cars They Made—Why Aren't They Doing Something about It?," *Volokh Conspiracy* (Jan. 10, 2014), http://www.volokh.com/2014/01/10/ford-knows-everyone-breaks-law-using-cars-made-arent-something.
[25] *Carpenter v. United States*, 585 U.S. ___(2018); *see also Carpenter v. United States*, EPIC, https://epic.org/amicus/location/carpenter/
[26] *Complaint of EPIC to the FTC against Uber*. [add link and fix cite]
[27] *See* EPIC, *Code of Fair Information Practices*, https://www.epic.org/privacy/consumer/code_fair_info.html.
[28] Proposed Framework at viii.

confidence in automated driving systems. This voluntary standard would also hinder effective oversight mechanisms that establish baseline safety protocols. EPIC urges DoT to implement mandatory safety and privacy protections for automated vehicles as soon as possible. Among other protections, DoT should include effective enforcement mechanisms to protect consumers from harms caused by noncompliance. EPIC recommends that DoT establish meaningful oversight mechanisms by providing a private right of action for consumers against companies who misuse or 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.[29] Without meaningful enforcement, consumers have no recourse if companies flout DoT's framework.

IV. The government has a critical role in developing cybersecurity best practices

Security is not only an issue in automated cars, but throughout the 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.[30] 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.[31] 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 and best practices are needed for all Internet of Things devices, but they are especially

[29] *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.
[30] *Blueprint for Cybersecurity Innovation*, AT&T, https://www.business.att.com/cybersecurity/cybersecurity-innovation/.
[31] *Id*.

necessary for vehicles. In order to be effective, these standards and best practices must be uniformly applied through government intervention.

Adoption and implementation of cybersecurity best practices is a critical measure to ensure uniform safety among automated vehicles, and the federal government should be involved. Data security should be built into vehicles.. To ensure automated vehicle safety and protect consumers' right to data security, DoT and other government agencies must assume greater responsibility and mandate cybersecurity best practices.

Since its inception in 1966, the Department of Transportation has helped promote public safety and protect the lives of Americans. In just over thirty years, DoT's regulation efforts helped cut motor-vehicle related deaths by half.[32] Because of the broad impact that DoT has made on vehicle safety to date, there is every reason to expect that the agency will play a pivotal in auto safety going forward. The agency should not defer to frameworks from other agencies, such as the Federal Trade Commission, that lack relevant expertise in auto safety and design. The FTC is not a data protection agency and has only limited authority in regulating privacy and data security as a Section 5 unfair or deceptive practice.[33] FTC enforcement authority has proven even more limited in effect.[34] Even if the FTC's regulatory powers were expanded, the agency still could not provide the cybersecurity expertise that automated cars require. The FTC cannot be relied upon to meaningfully guide nor enforce automated car constituents' data security practices. Instead, DoT is in the best position to establish and oversee implementation of cybersecurity best practices. As such, the

[32] *Morbidity and Mortality Weekly Report*, Department of Health and Human Services (2001), https://www.cdc.gov/mmwr/preview/mmwrhtml/mm4818a1.htm#fig2.
[33] 15 U.S.C. § 45(a)(1).
[34] *See e.g. Statement of EPIC to the Senate Commerce Committee on Oversight of the Federal Trade Commission*, Nov. 26, 2018, https://epic.org/testimony/congress/EPIC-SCOM-FTCOversight-Nov2018.pdf; *In re Uber Privacy Policy*, EPIC, https://epic.org/privacy/internet/ftc/uber/; *Complaint of EPIC to the Federal Trade Commission In re matter of WhatsApp, Inc.,* Aug. 29, 2016, https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf; Privacy? Proposed Google/DoubleClick Merger, EPIC, https://epic.org/privacy/ftc/google/.

Proposed Framework should be modified to make clear that the Department of Transportation is responsible for the privacy and security standards of vehicles in the United States,

Conclusion

Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0) lacks key recommendations to safeguard Americans in the era of connected vehicles. The Proposed Framework neither addresses the breadth and severity of safety risks posed by automated vehicles, nor adequately considers consumers' rights to privacy within the objective to protect American freedoms. Voluntary safety guidance also ignores the current risk of remote hacking and will impede efforts to make automated vehicles safer and more secure. In order to effectuate DoT's mission to promote public safety and protect American freedoms, the Department of Transportation must revise the Proposed Framework. While new vehicle technologies offer a variety of beneficial services to American drivers, these technologies also raise substantial privacy and safety concerns that must be addressed through comprehensive, legally enforceable safeguards. The Department of Transportation is the federal agency responsible for safeguarding American drivers. It cannot ignore the importance of this work.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Christine Bannan
Christine Bannan
EPIC Consumer Protection Counsel

/s/ Spencer K. Beall
Spencer K. Beall
EPIC Administrative Law Fellow