CENTER FOR DEMOCRACY & TECHNOLOGY

November 22, 2016

Docket Management Facility
U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building Ground Floor, Room W12-140
Washington, D.C. 20590-001

Re: Notice and Request for Comments on Federal Automated Vehicles Policy
NHTSA Docket No. 2016-0090-0001

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the National Highway Traffic Safety Administration's (NHTSA) request for comment on its Federal Automated Vehicles Policy. CDT is a nonprofit technology advocacy organization dedicated to promoting democratic values online, including digital privacy, free expression, and individual liberty. CDT recognizes the tremendous societal benefits that may be derived from autonomous technologies. Automated vehicles (AV) have the potential to expand access to transit for millions of Americans who struggle with adequate and affordable transportation, and for the elderly and the physically challenged population.[1] They also have the potential to improve fuel economy,[2] reduce accidents,[3] and reduce congestion.[4] For this potential to be achieved, however, NHTSA and other government agencies must address some of the significant technical and policy challenges these technologies pose.[5]

CDT applauds NHTSA's policy leadership in the deployment of AV technologies, and we encourage NHTSA to further explore the privacy and cybersecurity impacts of AVs. Specifically, these comments focus on the Federal Automated Vehicles Policy's Cross-Cutting Guidance with respect to: (1) data sharing; (2) privacy; (3) cybersecurity; and (4) consumer education and training.

---

[1] Stephanie Beasley, *Older, Disabled Drivers Pose Challenge for Driverless Car Makers*, Bloomberg BNA (May 6, 2016), http://www.bna.com/older-disabled-drivers-n57982070757/.

[2] Julia Pyper, *Self-Driving Cars Could Cut Greenhouse Gas Pollution*, Scientific American (Sept. 15, 2014), https://www.scientificamerican.com/article/self-driving-cars-could-cut-greenhouse-gas-pollution/.

[3] Michelle Fox, *Self-Driving Cars Safer Than Those Driven by Humans*, CNBC (Sept. 8, 2014), http://www.cnbc.com/2014/09/08/self-driving-cars-safer-than-those-driven-by-humans-bob-lutz.html.

[4] Peter Wayner, *How Driverless Cars Could Turn Parking Lots into City Parks*, Atlantic (Aug. 5, 2015), http://www.theatlantic.com/technology/archive/2015/08/driverless-cars-robot-cabs-parking-traffic/400526/.

[5] Apratim Vidyarthi, *Self-Driving into the Future: Putting Automated Driving Policy in Top Gear*, Ctr. for Democracy & Tech. (Aug. 9, 2016), https://cdt.org/blog/self-driving-into-the-future-putting-automated-driving-policy-in-top-gear/.

I. Data Sharing

The Policy rightly recognizes that sharing information with NHTSA and among members of the AV ecosystem will be an important tool to improving the safety benefits of AVs, addressing cybersecurity challenges, and enhancing consumer confidence in AV technologies generally. However, ensuring that data sharing is done appropriately, with due regard for drivers' privacy, is frequently contentious and challenging for the public sector.[6] Data sharing, by its nature, encourages the collection of more data, and while companies may be incentivized to protect business critical information, data sharing programs must be properly tailored to ensure they do not defeat efforts to encourage data minimization and deletion procedures.

While the Policy frames industry data sharing efforts as voluntary, it is conceivable that NHTSA's collection, retention, and sharing guidance will become mandatory over time. Voluntary information requests from government can lack oversight and necessary public transparency. CDT recommends that NHTSA provide additional guidance specifically as to how Safety Assessment information and other AV data shared with NHTSA will be collected, used, and securely stored.

A. Data Sharing Initiatives Need Appropriate Standards and Clear Use Limitations

As the Policy notes, there is currently a lack of consensus around appropriate data sharing standards, retention periods, and where and when companies are permitted to retrieve information from AVs. The Policy currently encourages industry to develop procedures for sharing "relevant data" in order to accelerate knowledge and understanding of AV technologies. Such broad, open-ended language for sharing among companies and with government agencies does not establish any clear limitations on what AV data may be shared or how it may subsequently be used. CDT is a strong proponent of specific use limits in the context of any information sharing proposal or initiative.

This is particularly important due to widespread variations in data retention policies and procedures across the automotive ecosystem.[7] Uncertain data retention periods expose information to the risk that an organization could weaken its internal controls, ownership is transferred, or the company could be dissolved or have its information assets liquidated.[8] Longer retention periods can also make data a

---

[6] Ctr. for Democracy & Tech., *Cybersecurity Information Sharing Bills Fall Short on Privacy Protections* (Apr. 22, 2015), https://cdt.org/insight/cybersecurity-information-sharing-bills-fall-short-on-privacy-protections/.

[7] GOV'T ACCOUNTABILITY OFFICE, GAO-14-81, IN-CAR LOCATION-BASED SERVICES: COMPANIES ARE TAKING STEPS TO PROTECT PRIVACY, BUT SOME RISKS MAY NOT BE CLEAR TO CONSUMERS (Dec. 6, 2013), http://www.gao.gov/products/GAO-14-81 [hereinafter GAO-14-81].

[8] Justin Brookman & G.S. Hans, *Why Collection Matters 5* (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf. The FTC has also highlighted concerns with data practices in light of bankruptcies and acquisitions. *See, e.g.*, Jamie Hine, Fed. Trade Comm'n, *Mergers and Privacy Promises* (Mar. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

target for malicious actors and increase the potential that information is subject to unauthorized access or accidental disclosure. On the other hand, the automotive industry also has legitimate reasons for retaining certain safety information for long periods of time. Automotive research and development cycles can last upwards of five years,[9] and certain data may need to be maintained in order to monitor vehicle models across the eleven-and-a-half-year average lifespan for most cars on the road.[10] CDT recognizes the challenges in resolving these competing mandates and encourages more discussion on establishing industry-wide retention standards for AV technologies.

Further, appropriate access levels, methods, formats, and timing of data sharing may vary based on the type of information at stake, and we believe much more thought must be given toward what categories of AV information can be appropriately shared. To address these issues, CDT supports NHTSA's suggestion that industry work with relevant standards bodies such as the IEEE and SAE to develop a uniform approach to data sharing with AV technologies.

B. More Research and Thinking Is Needed Around De-identifying AV Data

While the Policy does recommend that any AV data that is shared with third parties be de-identified, it is unclear what constitutes de-identified data from automated vehicles. NHTSA states that de-identified data is data that is stripped of elements that make it either directly *or* reasonably linkable to a specific AV owner or user. This definition embodies concepts supported by both the White House Consumer Privacy Bill of Rights[11] and the Federal Trade Commission's (FTC) understanding of personal data.[12] Linkability is obviously important to determining whether a dataset is properly de-identified, and while the efficacy of de-identification continues to be debated amongst researchers,[13] the vast array of data generated in both modern motor vehicles and emerging AV technologies raise new questions about which data elements could suffice to make information reasonably linkable or might serve as indirect identifiers.

---

[9] GOV'T ACCOUNTABILITY OFFICE, GAO-16-350, VEHICLE CYBERSECURITY: DOT AND INDUSTRY HAVE EFFORTS UNDER WAY, BUT DOT NEEDS TO DEFINE ITS ROLE IN RESPONDING TO A REAL-WORLD ATTACK 3 (Mar. 24, 2016), http://www.gao.gov/products/GAO-16-350 [hereinafter GAO-16-350].

[10] Nathan Bomey, *Average Age of Cars on U.S. Roads Breaks Record*, USA Today (July 29, 2015), http://www.usatoday.com/story/money/2015/07/29/new-car-sales-soaring-but-cars-getting-older-too/30821191/.

[11] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[12] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[13] *Compare* Arvind Narayanan & Edward W. Felton, *No Silver Bullet: De-identification Still Doesn't Work* (July 9, 2014), *with* Ann Cavoukian & Daniel Castro, Big Data and Innovation, *Setting the Record Straight: De-identification Does* Work (2014).

For example, researchers have shown that it is possible to accurately identify drivers using limited amounts of sensor data collected from existing vehicles on the road. Drivers could be identified with 87% accuracy, using only the positioning of the brake pedal after monitoring fifteen minutes' worth of driving; the number jumped to 99% accuracy when access was granted to additional driving behavior and sensor data.[14] Like similar sorts of digital fingerprinting based upon device or browser settings, an "automotive fingerprint" can be derived based on individual driver patterns or vehicle usage. Because of this, sharing AV data in a privacy protective manner will be complex. While it is true that the identifiability of drivers' fingerprint may diminish as AVs attain higher levels of autonomy, data sharing efforts will present a privacy and data security threat model that will evolve over time.[15]

Moreover, it is also unclear the effectiveness of the industry's application of de-identification methods. A study by the Government Accountability Office (GAO) on in-car location based services found that automakers and navigation service providers were using different de-identification methods. The study concluded that this variation in de-identification methods could impact the extent to which consumers could be easily re-identified or otherwise exposed to privacy risks.[16] Industry should explore whether and how it can go beyond simply stripping away direct and indirect identifiers from AV data. One potential suggestion that has been highlighted is to explore the use of differential privacy.[17] Considering the potential volume of information that might be generated by AV technologies, differential privacy techniques could be useful in instances where raw, individualized AV data is not needed. By adding statistically insignificant amounts of noise to data, differential privacy could permit researchers to query a dataset while protecting the disclosure of information related to any one individual.[18]

C. Existing Consumer Notice and Education Should Be Improved

CDT agrees that automakers and other entities in the AV ecosystem must only share data in accordance with their existing privacy policies and the terms of services that are provided to consumers and dealers. However, as we discuss in further detail below, informing consumers about data collection, use, and sharing through lengthy policies is not ideal. Effective notice of data sharing arrangements with AVs will require additional consumer education and information. Based on the

---

[14] Miro Enev et al., *Automobile Driver Fingerprinting*, Proceedings on Privacy Enhancing Technologies (2016).

[15] *Id.*

[16] GAO-14-81, *supra* note 7, at 20.

[17] *See* Brian Fung, *A Privacy Policy for Cars*, Wash. Post (Dec. 9, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/09/a-privacy-policy-for-cars-what-automakers-know-about-you-and-what-theyre-doing-with-it/.

[18] Greg Norcie, *Think Differentially: Apple's Forward-Thinking Approach to Privacy in iOS 10,* Ctr. for Democracy & Tech. (June 29, 2016), https://cdt.org/blog/think-differentially-apples-forward-thinking-approach-to-privacy-in-ios-10/; *see also* Simson L. Garfinkel, *De-Identification of Personal Information*, Nat'l Inst. of Standards & Tech. (2005), available at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

industry's existing track record with respect to communicating data practices[19] and cybersecurity incidents[20] to consumers, additional transparency efforts and more effective communication will be essential to promote consumer trust.

II. Privacy

The ramifications of AV technologies for driver privacy should not be taken lightly. Forty-five percent of new car buyers are concerned about the privacy impacts of new in-car technologies.[21] While the automotive industry has not traditionally had access to the stream of digital information available to other consumer-facing industries, connectivity presents ample opportunities for industry to engage in driver monitoring and highly tailored marketing.[22] In light of the potential for AV technologies to invade driver privacy, CDT is pleased to see that the Policy recommends that both automakers and other entities in the AV ecosystem take proactive steps to protect consumers' privacy.

A. Existing Guidance Does Not Capture AV Privacy Concerns

As a baseline, the Policy suggests that organizations guide their policies and practices by embracing the longstanding Fair Information Principles (FIPs) as expressed in the White House Consumer Privacy Bill of Rights and in existing FTC guidance. The Policy also highlights a set of "Privacy Principles for Vehicle Technologies and Services" that was adopted by nineteen automakers in 2014 as a potential resource to guide the AV ecosystem.[23] While CDT believes that the FIPs should form the basis for how industry and government alike approach AV data collection and use, it is important to acknowledge that neither the Privacy Bill of Rights nor the industry's Privacy Principles comprehensively address the privacy concerns that exist with regard to AVs.

These documents are largely generalized privacy frameworks rather than legal guidance. For example, the Privacy Bill of Rights provides a high-level framework for thinking about how to address consumer privacy, but it does not establish any binding requirements on the AV ecosystem. As a public

---

[19] Jim Edwards, *Ford Exec Retracts Statements About Tracking Drivers With The GPS In Their Cars*, Business Insider (Jan. 9, 2014), http://www.businessinsider.com/ford-jim-farley-retracts-statements-tracking-drivers-gps-2014-1.

[20] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, Wired (July 24, 2015), https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[21] McKinsey & Co., *What's Driving the Connected Car?*, http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car (last visited Nov. 15, 2016).

[22] RICHARD VIERECKL ET AL., PWC, CONNECTED CAR REPORT 2016 (Sept. 28, 2016), http://www.strategyand.pwc.com/reports/connected-car-2016-study (PwC's report encourages companies to "use your data," calling it "an opportunity not to be missed.").

[23] Consumer Privacy Protection Principles, Alliance of Automobile Manufacturers (Nov. 12, 2014), *available at* http://www.automotiveprivacy.com [hereinafter Privacy Principles].

commitment from automakers, the Privacy Principles are legally enforceable by the FTC under the Commission's Section 5 authority to police deceptive business practices, but the Privacy Principles currently apply only to the nineteen companies that have signed onto them. They do not apply to vehicle dealerships, insurers, or aftermarket suppliers and may not be applicable to various third party service providers that work with automakers.[24] As a result, a significant portion of the AV ecosystem is not covered by the Privacy Principles, and as automakers work with startups and other technology companies on AV technologies, the Privacy Principles' scope will be further limited.

B. Affirmative Requirements of Automotive Privacy Principles Are Unclear

Also, while the Privacy Principles affirm the high-level principles embodied in the Privacy Bill of Rights,[25] they provide limited guidance as to how automakers should implement them in practice. For example, the Privacy Principles were designed to help promote transparency about vehicle data practices, and they oblige automakers to provide clear and meaningful notice about data practices. Effective notice of the implications of connectivity for drivers' privacy is essential, but the language of the Privacy Principles generally encourages longer and more confusing policy documents and terms of service.[26] While automakers were encouraged to provide information through means other than online privacy policies – and Toyota, for example, provides a dedicated web portal that describes the privacy practices of its connectivity features[27] – data practices continue to be conveyed primarily via unclear privacy policies.

Clear and meaningful notice is particularly important because of how the Privacy Principles direct automakers to respect the context in which information is collected. While this principle generally requires organizations only to use information in ways that are consistent with consumer expectations at the point of collection, the Privacy Principles deem this concept to be satisfied if uses are explained in a privacy policy rather than embedded in the company's data practices.[28] Respect for context should go beyond the four corners of a privacy policy. An individual's contextual expectations rest on a number of subjective variables such as an individual's level of trust in an organization and her

[24] "Participating Members commit to taking reasonable steps to ensure Third-party Services Providers adhere to the Principles . . . . However, the Principles directly apply only to Participating Members." *Id.*

[25] Specifically, manufacturers affirm the following fundamental principles of transparency; choice; respect for context; data minimization, de-identification, and retention; security; integrity and access; and accountability.

[26] BC FREEDOM OF INFO. & PRIVACY ASSOC., THE CONNECTED CAR: WHO IS IN THE DRIVER'S SEAT? 94 (2015), https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf.

[27] Toyota Connected Vehicles Services Privacy and Protection Web Portal, http://www.toyota.com/privacyvts/ (last visited Nov. 15, 2016).

[28] Privacy Principles, *supra* note 23, at 9: "When Participating Members present clear, meaningful notices about how Covered Information will be used and shared, that use and sharing is consistent with the context of collection."

perception of the value she might receive from the use of her information.[29] When the concept of respect for context is only embraced in principle and not practice, it becomes susceptible to a number of competing determinations.[30] Traditionally, drivers have understood the interior of their vehicles to be a private space, but connectivity makes the driving experience transparent to a growing number of third parties of which the driver is unaware. Consumer interaction with AV technologies will further alter the consumer's relationship with her vehicle, changing existing social and cultural expectations in any given car ride. This changing dynamic suggests that being respectful of context will require companies to do more than provide notice.

Third, while the NTSHA Policy recommends that automakers offer drivers choices regarding the collection, use, sharing, retention, and deconstruction of their personal data, the Privacy Principles promulgated by automakers are weaker. For example, they do not require automakers to provide users with data sharing options when the information being collected or used is for safety, operations, or compliance purposes.[31] The sphere of vehicle functionality that is captured by this exception will only grow as vehicles add automated technologies and connectivity features. Tesla, which is not a signatory to the Privacy Principles, explains that failure to share vehicle data result in not just reduced functionality but serious damage or inoperability.[32] In effect, consumers are forced to consent to sharing their data as a condition of buying a new car, which is hardly a meaningful choice. When the Privacy Principles were first announced, automakers suggested that individual companies would compete on privacy, and features such as a "private driving mode" akin to a private web browsing were offered as one potential mechanism.[33] NHTSA should encourage industry to explore such functionality as AV technologies are incorporated into more product lines. If drivers are not provided suitable controls over their information, specific restrictions on how industry uses AV data may be needed.

Fourth, as addressed above, there are no standards for how AV data should be de-identified. The Privacy Principles state only that information should be de-identified but do not detail acceptable or effective methods, and automakers may have different interpretations of what may be considered outside the scope of protected information. For example, OnStar's privacy policy does not apply to

---

[29] Carolyn Nguyen, Director, Microsoft Technology Policy Group, Contextual Privacy, Address at the FTC Internet of Things Workshop (Nov. 19, 2013), *available at:* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connectedworld/final_transcript.pdf.

[30] *See* Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't*, Berkeley Law (May 24, 2013, 9:31 PM), http://privacylaw.berkeleylawblogs.org/2013/05/24/helen-nissenbaum-respect-for-context-as-a-benchmark-for-privacy-online-what-it-isand-isnt-2/.

[31] Privacy Principles, *supra* note 23, at 8-9. *See also* Gilad Rosner, *There Is Room for Global Thinking in IoT Data Privacy Matters*, O'Reilly (Feb. 4, 2015), https://www.oreilly.com/ideas/there-is-room-for-global-thinking-in-iot-data-privacy-matters.

[32] Tesla, Customer Privacy Policy, https://www.tesla.com/about/legal (last updated Sept. 2016).

[33] Fung, *supra* note 17.

"anonymized information" that "no longer reasonably identifies you or your vehicle."[34] Ford's SYNC permits the unrestricted use and sharing of "aggregate (non-personally identifiable) information,"[35] and Toyota Safety Connect has different rules for categories of personal information and vehicle data.[36] These policies do not provide any light into which vehicle data elements may or may not be identifying, and as the GAO reported, it is likely that companies are using different de-identification methods and standards.

III. Cybersecurity

Cybersecurity is a critical in AVs.[37] The security challenge presented by AV technologies is compounded by the security risks inherent in existing automotive systems.[38] The Control Area Network (CAN) is a centralized vehicle communication network that was designed approximately thirty years ago, and remote security was logically not a priority in its development. As a result, automotive security research remains in its infancy, and serious security vulnerabilities in existing automotive systems have only been widely recognized since 2010.[39] By 2015, researchers demonstrated that remote attacks against production vehicles were possible by using the connectivity features in a 2014 Jeep Cherokee to disable the vehicle's brakes and, in certain circumstances, take over its steering.[40] After receiving widespread public attention, Fiat Chrysler Automobiles ultimately recalled 1.4 million vehicles in order to implement a software patch.[41]

The incorporation of AV technologies on top of legacy automotive architectures will present new threat vectors. AVs present a massive attack surface: the average vehicle on the road today has

---

[34] OnStar Privacy Statement - Summary, https://www.onstar.com/us/en/footer-links/privacy-policy.html (last visited Nov. 15, 2016).

[35] SYNC Terms & Conditions of Use, https://owner.ford.com/tools/account/sync-terms-and-conditions.html (last updated Aug. 3, 2016).

[36] Toyota, *supra* note 26.

[37] *See* Alex Webb, *Cybersecurity Is Biggest Risk of Autonomous Cars, Survey Finds*, Bloomberg Tech. (July 19, 2016), https://www.bloomberg.com/news/articles/2016-07-19/cybersecurity-is-biggest-risk-of-autonomous-cars-survey-finds; Nathaniel Mott, *As Self-Driving Cars Hit the Road, Cybersecurity Takes a Back Seat*, CSM Passcode (Oct. 13, 2016), http://www.csmonitor.com/World/Passcode/2016/1013/As-self-driving-cars-hit-the-road-cybersecurity-takes-a-back-seat.

[38] Hiawatha Bray, *After Car Hack, Internet of Things Looks Riskier*, betaBoston, Boston Globe (Aug. 3, 2015), http://www.betaboston.com/news/2015/08/03/after-car-hack-internet-of-things-looks-riskier/. For a detailed discussion of recent research into automotive security vulnerabilities, including the CAN bus, see Roderick Currie, *Developments in Car Hacking*, SANS Reading Room (Dec. 5, 2015), https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607.

[39] Currie*, supra* note 38, at 15.

[40] CHARLIE MILLER & CHRIS VALASEK, REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE (Aug. 10, 2015), *available at:* http://illmatics.com/Remote%20Car%20Hacking.pdf.

[41] Chris Bruce, *FCA Issuing Software Update for 1.4M Vehicles to Prevent Hacking*, Autoblog (July 24, 2015), http://www.autoblog.com/2015/07/24/fca-software-update-prevent-hacking-recall/.

upwards of a 100 separate electronic control units (ECUs) that monitor and control individual vehicle systems, and these systems are comprised of millions of lines of code.[42] Due to the interconnected nature of ECUs, the security of safety-critical ECUs depends upon the security of other ECUs.[43] The entrance of vehicle-to-vehicle and vehicle-to-infrastructure technologies to facilitate automated functionality may further increase this cybersecurity interdependence, and vehicle security may depend upon the security protocols and practices of numerous other entities.

A. Supply Chain Management and Security Collaboration Should Be Prioritized

The Policy properly suggests that automakers insist that their vendors and suppliers build robust security features into their equipment, but the complexity of the automotive ecosystem and the introduction of aftermarket functionality and plug-in "dongles" may prove a daunting challenge. Further, automakers presently source ECUs from many different automotive suppliers, which suggests that no one entity controls a vehicle's source code.[44] A cybersecurity study from the GAO reported that automotive stakeholders frequently cite "the lack of transparency, communication, and collaboration regarding vehicles' cybersecurity" among automakers and suppliers as a primary security concern.[45] Moreover, cybersecurity vulnerabilities are frequently discovered at interfaces where software code written by different suppliers must interact.[46]

The auto industry has had challenges at effective collaboration due to a combination of historical factors and a competitive environment. Deploying and securing AVs will require additional dialogue (1) within the auto industry and (2) with outside parties, especially security researchers. One avenue for such dialogue could be the nascent Automotive Information Sharing and Analysis Center (Auto-ISAC). The Auto-ISAC has made great strides in short time, releasing a framework for automotive cybersecurity best practices in January and announcing in July that it had established a set of industry best practices. It also recognizes the need to collaborate and engage with "appropriate third parties."[47] While the Auto-ISAC's immediate membership should be expanded to include suppliers and other AV

---

[42] 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.

[43] Mark S. Sherman & Jens Palluch, *Cybersecurity Considerations for Vehicles* (Dec. 2015), *available at*: https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_448313.pdf.

[44] Robe Toews, *The Biggest Threat Facing Connected Autonomous Vehicles Is Cybersecurity*, TechCrunch (Aug. 25, 2016), https://techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/.

[45] GAO-16-350, *supra* note 9, at 3.

[46] *Id.* at 26.

[47] Automotive Cybersecurity Best Practices, Executive Summary, Auto-ISAC (July 2016), https://www.automotiveisac.com/best-practices/.

technology companies, engagement and collaboration with other entities, specifically independent security researchers, will be essential, as well.

NHTSA has an important ongoing role in bridging tensions that exist among the auto industry and security researchers generally.[48] The Proactive Safety Principles that were released in partnership among NHTSA, the Department of Transportation, and eighteen automakers recognized the importance of engaging with independent security researchers to address cybersecurity vulnerabilities in vehicles.[49] Proactive activities such as "bug bounty" programs are positive developments, but the auto industry has also taken policy positions that would have criminalized valuable security research under both the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act. These efforts are counterproductive considering industry's hesitation to embrace binding security requirements on its own.

B. NHTSA Must Work with Other Federal Regulators on Security and Privacy

Regulatory collaboration for AVs is particularly warranted given NHTSA's broad but limited mandate to address vehicle safety; it is possible that effectively monitoring the cybersecurity of AVs is beyond the resource-constrained capabilities of NHTSA alone.[50] NHTSA has said that any determination on binding cybersecurity standards will not happen until 2018. Without binding rules, it is likely that other cybersecurity regulators may step in to promote a security baseline for certain AV technologies. Industry best practices could be used to establish what constitutes reasonable data security by the FTC, and automakers and others' failure to meet those practices would then constitute an unfair business practice. Additionally, the FCC is currently considering a potential rulemaking to establish privacy and security standards for drivers in DSRC-enabled vehicles, and the FCC has indicated that a number of interrelated issues presented by vehicle connectivity warrant collaboration with NHTSA.[51] It behooves NHTSA to establish a more formal relationship with other federal regulators with dedicated privacy and cybersecurity expertise.

---

[48] Andy Greenberg, *Feds Prod Automakers to Play Nice with Hackers*, Wired (Jan. 15, 2016), https://www.wired.com/2016/01/feds-prod-automakers-to-play-nice-with-hackers/;
Pete Bigelow, *Automakers Again at Odds with Cyber-Security Researchers*, Autoblog (July 15, 2015), http://www.autoblog.com/2015/07/15/automakers-isac-car-hack-cyber-security-congress/.

[49] Proactive Safety Principles (Jan. 15, 2016), https://www.transportation.gov/briefing-room/proactive-safety-principles-2016.

[50] Statement of Laura MacCleery, Vice President, Consumer Policy and Mobilization, Consumer Reports Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade (Nov. 15, 2016), *available at:* http://docs.house.gov/meetings/IF/IF17/20161115/105416/HHRG-114-IF17-Wstate-MacCleeryL-20161115.pdf. *See also,* Gelles, *supra* note 42 ("The agency estimates that it has 0.3 staff members for every 100 fatalities in automobile crashes; the F.A.A. has at its disposal over 10,000 staff members for every 100 fatalities on commercial aircraft, according to N.H.T.S.A.").

[51] Letter from Tom Wheeler, FTC Chairman, to Sens. Richard Blumenthal and Edward Markey (Sept. 7, 2016), available at: https://apps.fcc.gov/edocs_public/attachmatch/DOC-341318A1.pdf.

IV. Consumer Education and Training

The Policy recognizes that consumer education and training will be essential to safely deploy AVs, and that an effective AV policy will also seek further input from consumers. While our comments have emphasized the privacy and cybersecurity concerns that could hamper consumer acceptance of AVs, consumer apprehension about the loss of control and autonomy that comes with AV technologies and accompanying new, shared ownership models must also be addressed.[52]

Even without the introduction of new AV technologies, the automotive ecosystem is a complex interrelationship among automakers, dealers, and suppliers. The model in which cars are sold to consumers creates different incentives for each of these parties, and as a result, clear and consistent communications with consumers about AV technologies and new automotive connectivity can be challenging. NHTSA must ensure that representative consumer voices are also heard as it revises and updates the Policy in the future.

Conclusion

Automated vehicles have tremendous potential to reshape the transportation landscape, and NHTSA's AV Policy provides a high-level roadmap for implementing AV technologies in a safe fashion. CDT encourages NHTSA to consider the privacy and security concerns highlighted in these comments and those noted by security researchers, consumer groups and consumers themselves.

NHTSA should move as quickly as possible to establish binding privacy rules and cybersecurity standards in AV technologies in order to promote consumer trust. In the interim, it should work with both industry and new stakeholders to address the technical and policy challenges posed by AVs.

Thank you for the opportunity to provide comments on NHTSA's Federal Automated Vehicles Policy. We welcome any questions or comments.

Sincerely,

Joseph Jerome
Policy Counsel
Center for Democracy & Technology

[52] Sascha Meinrath & Georgeta Dragoiu, *Opinion: Driverless Cars Need an Off Switch*, CSM Passcode (Oct. 12, 2016), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/1012/Opinion-Driverless-cars-need-an-off-switch.