March 20, 2018

National Highway Traffic Safety Administration
West Building, Ground Floor
Room W12-140
1200 New Jersey Avenue, S.E.
Washington, District of Columbia 20590

*Re: Removing Regulatory Barriers for Vehicles with Automated Driving Systems, Docket No. NHTSA-2018-0009*

## I. Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to provide comments to the National Highway Traffic Safety Administration (NHTSA) in its proceeding on the removal of barriers to promote the deployment of vehicles with automated driving systems (ADS).[1]

The App Association represents more than 5,000 small business app developers and technology firms across the United States and throughout the mobile economy. Our members have developed innovative applications and products that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. Today, the app ecosystem is worth more than $143 billion and is a key driver of the $8 trillion internet of things (IoT) revolution.[2] In our State of the App Economy report, we explore how the ever-evolving IoT ecosystem impacts companies, even those unaffiliated with the information and communication technology sector.[3] Many of our members supply the "middleware" that connects IoT devices, including connected vehicles.

[1] Removing Regulatory Barriers for Vehicles with Automated Driving Systems, Docket No. NHTSA-2018-0009, Request for Comment, 83 F.R. 12 (2018).

[2] State of the App Economy, ACT | The App Association 2, 5th ed. (2017). Available at: http://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf.

[3] See id.

The advent of ADS-enabled vehicles will lead to safer driving conditions and more efficient means of conveyance. NHTSA found that more than 35,000 Americans lost their lives in auto collisions in 2015, which was a 7.2 percent increase from the previous year. Sadly, many car accidents are a result of human error, with distracted drivers representing one of the leading causes in "human choice" crash situations.[4] In 2016, the auto-related fatalities rose 5.6 percent.[5] ADS-enabled vehicles have the unique potential to reduce this public safety concern. Our members, along with auto manufacturers, original equipment managers (OEMs), and others will play an important role in ensuring these vehicles are safe and effective.

## II. NHTSA Should Enable Manufacturers and OEMs to Leverage Software Application Innovations

Over the years, apps have demonstrated a strong ability to introduce new efficiencies and innovations across myriad of economic verticals and will play a role in interior and exterior vehicular designs and developments in ADS vehicles. It is crucial that NHTSA's Federal Motor Vehicle Safety Standards (FMVSS) allow app-based innovations to grow in the automotive space. As this Request for Comment recognizes, the advent of ADS-enabled vehicles and their app-driven interfaces will change the driving experience for all riders.

Consumer demand for apps has already influenced the interior and exterior designs of vehicles, and this increased use of apps on popular mobile platforms like Android's Google Play and the Apple App Store has significantly impacted the integration of apps into connected vehicles. Today more than 40 automakers are selling 100 car models equipped with Apple's CarPlay, which affixes a dashboard panel that mirror a smartphone.[6] CarPlay also supports apps on your iPhone and allows consumers and drivers to organize their apps' presentation on their car dashboard.[7] CarPlay seamlessly integrates your phone into your car. The simple presence of your phone (or another passenger's) plays your podcasts, reads your maps, and even reads your texts to you.

---

[4] See id.

[5] 2016 Fatal Traffic Crash Data, U.S. Dep't of Transp. (Oct. 6, 2017). Available at: https://www.nhtsa.gov/press-releases/usdot-releases-2016-fatal-traffic-crash-data.

[6] Tuan Huynh, Apple CarPlay: Everything You Need to Know About iOS in the Car, Techradar (Jun. 5, 2017). Available at https://www.techradar.com/news/car-tech/apple-carplay-everything-you-need-to-know-about-ios-in-the-car-1230381.

[7] CarPlay, Apple. Available at: https://www.apple.com/ios/carplay/.

App developers are already creating software solutions in the ADS space. For example, Bosch is developing an automated valet parking (AVP) system that allows drivers to use a smartphone app to drop off their cars at a specified location to be self-parked.[8] The app shares data between the drop point and the parking garage to calculate the route to an available parking space. The driver can then use the app to retrieve their car. In another example, Lyft and Ford have collaborated to develop a ride app for AVs that uses Lyft's app to communicate with Ford cars.[9]

App developers have presented another solution in Lvl5's Payver, which is developing detailed maps that will provide enough data for AVs to identify the precise location of traffic lights, curbs, stop signs, and many other landmarks.[10]

We believe NHTSA's policies should allow ADS manufacturers to leverage innovative solutions from third party apps into autonomous vehicles. The "launch fast and iterate"[11] nature of app companies has enabled the app ecosystem to evolve and adapt around market shifts, creating new opportunities for users. However, NHTSA's proposal of a one-size-fits-all rule for ADS vehicles and components could stifle innovation and dissuade participation in this dynamic industry. We welcome NHTSA's effort to establish effective rulemaking procedures to secure passenger safety in ADS vehicles, but we caution against NHTSA applying its safety evaluation process in a one-size-fits-all fashion because that would unduly impede ADS deployment.

We urge NHTSA to build upon the experiences of other U.S. federal sector-specific agencies who have carefully grappled with the role of software and its transformative role in safety-of-life products and services. For example, the U.S. Food and Drug Administration's (FDA) recent adoption of a scalable and risked-based evaluation framework to determine the regulations it will impose on health software, is a commendable effort to encourage the integration of innovative technology and promote the safety of the user.[12] As a further example, the FDA has stated that changes made to devices solely to strengthen cybersecurity, or to return a system into specification of a

---

[8] Automated Valet Parking: Parting at the touch of a button, Bosch. Available at: https://www.bosch-mobility-solutions.us/us/highlights/automated-mobility/automated-valet-parking/.

[9] Andrew J. Hawkins, Ford and Lyft will work together to deploy autonomous, The Verge (Sept. 27, 2017). Available at: https://www.theverge.com/2017/9/27/16373574/ford-lyft-self-driving-car-partnership-gm.

[10] Alex Davies, Wanna Help Self-Driving Cars? Turn on Your Phone's Camera, WIRED (July 19, 2017). Available at: https://www.wired.com/story/wanna-help-self-driving-cars-turn-on-your-phones-camera/.

[11] To launch fast and iterate is often used to describe a software developer's business plan, where software developers like to launch products as soon as they are finished and like to update newer iterations of their product actively. Paul Graham, Apple's Mistake, paulgraham.com (Nov. 2009) Available at: http://www.paulgraham.com/apple.html.

[12] Mobile Medical Device Applications, FDA. Available at: https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm

more recently-approved device, will not trigger a full re-approval of that medical device.[13] Even more recently, the FDA launched a Digital Health Software Precertification Program to streamline regulations to accommodate emerging healthcare software.[14] Such approaches have provided the small business software developer community with much-needed clarity about FDA regulations that will apply to their software.

The App Association respectfully urges NHTSA to consider how it can leverage the small business software development community, while protecting passenger safety, particularly when OEMs incorporate emerging technologies developed by third party app developers into autonomous vehicles. For instance, NHTSA should permit non-passenger safety software updates to ADS and it should minimize the burden on its approval processes on small business innovators. We hope NHTSA's processes facilitate an environment where our members and other app developers can bring innovative solutions to OEMs and car manufacturers to realize the full potential of ADS vehicles.

## III. NHTSA Should Promote Risk-Based Cybersecurity Threat Mitigation Approaches for AVs

We applaud NHTSA for using the Department of Commerce's National Institute of Standards and Technology (NIST) as a foundation and resource for cybersecurity infrastructure for vehicles.[15] We believe the NIST framework will inform NHTSA of our commitment to ensure the integrity of cybersecurity systems in ADS vehicles.

While the rise IoT holds great promise, it also raises security threats. Due to a broadened attack vector, the growth of IoT will require more dynamic risk management practices. Our members appreciate the personal value of their customers' data and put extensive resources into ensuring its privacy and security.

---

[13] Deciding When to Submit a 501(k) for a Software Change to an Existing Device, FDA (Oct. 25, 2017). Available at: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm514737.pdf

[14] Digital Health Software Precertification (Pre-Cert) Program, FDA. Available at: https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/default.htm

[15] E.g., National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333). Washington, DC. Available at file:///Users/joelthayer/Downloads/812333_CybersecurityForModernVehicles.pdf.

We support public-private partnership initiatives to improve the United States' cybersecurity risk management efforts and continue to work with our members to advance cybersecurity risk management practices. Small businesses represent 99.7 percent of American companies[16] and must play a more significant role in the development of cybersecurity risk strategies. While large companies can dedicate large budgets to develop cybersecurity control processes or hire staff to mitigate cybersecurity risks, small and medium-sized enterprises often do not have the resources to do the same. In fact, in many small businesses, the role of chief security officer may be one of five hats worn by a single employee. For this reason, the NIST Cybersecurity Framework is even more vital to the security and stability of the nation's critical infrastructure.

We believe the NIST Cybersecurity Framework should be the touchstone to enhance private sector cybersecurity efforts in the automotive space. NHTSA's rules should include references to the Framework but should not mandate its application too granularly. The Framework is a toolbox intended to be used in a scalable way appropriate for each individual company's risk. NHTSA should also provide references to related resources for SMEs, such as NIST's *Small Business Information Security: The Fundamentals*[17] and the Federal Trade Commission's (FTC) *Start with Security* guide for SMEs.[18] We commit to work closely with NHTSA and other public and private stakeholders to develop and help implement more small business-focused cybersecurity risk management practices that support the role of apps in advanced vehicular solutions.

Lastly, we would like to call attention to Congress' introduction of the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution (SELF DRIVE) Act, which attempts to ameliorate cybersecurity concerns in ADS vehicles by requiring manufacturers of self-driving cars to submit safety assessment certifications.[19] The bill would update and clarify NHTSA's role in the development of cybersecurity practices and would be a welcomed framework as vehicles enter levels 4 and 5 of automation. The App Association hopes that NHTSA will try to adopt this framework under the limits of current legal jurisdiction.

---

[16] Frequently Asked Questions, SBA Office of Advocacy (Sept. 2012). Available at: https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.

[17] Small Business Information Security: The Fundamentals, NISTIR 7621, Revision 1 (Nov. 2016). Available at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[18] Start with Security: A Guide for Business, FTC. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[19] See H.R. 3388.

## IV. Conclusion

The App Association appreciates the opportunity to express our views on this important issue. We hope these comments and suggestions will be helpful to NHTSA in the development of this proceeding.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Policy Counsel

McKenzie Schnell
Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005