ITS AMERICA

Intelligent Transportation Society of America
1100 New Jersey Ave., SE, Ste. #850
Washington, DC 20003

PH 202.484.4847
FX: 202.484.3483
www.itsamerica.org

July 31, 2017

Via Electronic Filing

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex A)
Washington, DC 20580

Re: Connected Cars Workshop and P175403

Dear Mr. Clark:

The Intelligent Transportation Society of America (ITS America)[1] is pleased to submit these comments to the Federal Trade Commission (Commission) in response to the agency's request for comments[2] on issues raised during the Commission's June 28, 2017, joint workshop with the National Highway Traffic Safety Administration (NHTSA) on "Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles."[3] ITS America appreciates this effort by the Commission and NHTSA to seek information from a broad range of stakeholders to discuss "issues related to connected and automated vehicles that collect data."[4]

I. The Importance of Intelligent Transportation

ITS America seeks to revitalize our infrastructure and modernize our outmoded transportation system. Broadly, we seek to improve the safety and efficiency of our transportation networks and our nation's economy, standard of living, and health and security. Transportation connects communities and

[1] The Intelligent Transportation Society of America (ITS America) is the nation's leading advocate for the technological modernization of our transportation system by focusing on advancing research and deployment of intelligent transportation systems. Its unique membership brings together all key stakeholders in the intelligent transportation movement—including established and emerging private companies, public agencies and state departments of transportation officials as well as leaders in the academic and research communities.

[2] Federal Trade Commission, *FTC and NHTSA Seek Input on Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicle*s, Mar. 20, 2017, *available at:* 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.

[3] Federal Trade Commission, *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, June 28, 2017, *available at:* https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected . ("*FTC/NHTSA Workshop*").

[4] *Id.*

is the lifeblood of commerce. It widens job opportunities and is essential to addressing equity, poverty, unemployment, and access to education and health care. We believe "intelligent transportation" can address the broadest spectrum of challenges and opportunities.

Our objective is to grow our economy and improve our quality of life through innovative technologies that enhance the mobility, safety, security, privacy, sustainability and accessibility of our transportation system in the next decade. Safety, security and privacy in particular are critical and must be addressed by the technology sector along the entire technology lifecycle—in design, development, deployment, and operations. ITS America seeks to grow collaboration within industry and between private and public sectors in these critical areas.

A. Fatalities as well as Congestion are Increasing on Our Nation's Roads

NHTSA estimates that human errors cause approximately 94% of all vehicle crashes.[5] NHTSA reported in 2016 that 35,092 people were lost in crashes on U.S. roadways during 2015—an increase from 32,744 in 2014.[6] The 7.2% increase is the largest percentage increase in nearly 50 years.[7] NHTSA also reported that the estimated number of people injured on our Nation's roads increased in 2015, rising from 2.34 million to 2.44 million injured people.[8]

This disheartening trend shows no sign of abating. Using preliminary data, NHTSA estimates that an estimated 27,875 people died in motor vehicle traffic crashes during the first nine months of 2016--an increase of about 8% as compared to same time period in 2015.[9] The third quarter of 2016 represents the eighth consecutive quarter with increases in fatalities.[10]

Besides the obvious impact on the individuals affected by these crashes, there also is an enormous societal and economic toll. A NHTSA study--using 2010 data--calculated that motor vehicle crashes costs Americans $871 billion per year, with $277 billion in economic costs and $594 billion in harm from the loss of life and the pain and decreased quality of life due to injuries.[11]

The economic harm of congestion on our nation's roads in 2016 to U.S. drivers has been estimated at $300 billion in direct and indirect costs--an average of $1,400 per driver, according to the

[5] NHTSA, *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Surve*y, Feb. 2015, *available at: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115*.

[6] NHTSA, *2015 Motor Vehicle Crashes: Overview*, Aug. 2016, *available at:* https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812318.

[7] *Id.*

[8] *Id.*

[9] NHTSA, *Early Estimate of Motor Vehicle Traffic Fatalities For the First 9 Months of 2016*, Jan. 2017, *available at: https://crashstats.nhtsa.dot.gov/Api/Public/Publication/812358*.

[10] *Id.*

[11] NHTSA, *New NHTSA Study Shows Motor Vehicle Crashes Have $871 Billion Economic and Societal Impact on U.S. Citizens*, May 28, 2014, *available at:* https://www.nhtsa.gov/press-releases/new-nhtsa-study-shows-motor-vehicle-crashes-have-871-billion-economic-and-societal.

INRIX Traffic Scorecard.[12] Another report found that congestion kept travelers in their cars for nearly seven billion extra hours--42 hours per rush-hour commuter--costing the U.S. economy $160 billion, or $960 per commuter.[13]

B. Vehicle-to-Everything (V2X) Communications Will Improve Traffic Safety and Overall Mobility on Our Nation's Roads

ITS America agrees with NHTSA Acting Executive Director Terry T. Shelton that automatic driving systems are a revolution in auto safety.[14] As noted in ITS America's policy public roadmap, intelligent transportation can save tens of thousands of lives each year and billion of dollars.[15] Specifically, vehicle-to-everything (V2X) communications allow vehicles to "talk" with each other, roadway infrastructure (e.g., intersections, on-ramps, and work zones), bicyclists, and pedestrians.

Dedicated Short Range Communications (DSRC) operating within the 5.9 GHz Safety Spectrum band is the critical link for V2X communications, enabling vehicles to have a 360 degree "view" of adjacent vehicles and roadside conditions that the driver cannot see. Example DSRC applications include: Blind Spot Warning, Forward Collision Warning, Lane Change Warning, Intersection Collision Avoidance, and Approaching Emergency Vehicle Warning, among others. Most significantly, DSRC is the only wireless data communications that has the requisite low latency--the time it takes data to reach its destination--with high reliability that is critical for the transmission of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) safety messages. ITS America is a founding member of the Safety Spectrum Coalition, a group formed to promote and protect the use of the 5.9 GHz band for DSRC and V2X applications.[16] Other industry groups also have voiced their support for the 5.9 GHz Safety Spectrum band.[17]

[12] INRIX, *Los Angeles Tops INRIX Global Congestion Ranking, Feb. 20, 2017, available at:* http://inrix.com/press-releases/los-angeles-tops-inrix-global-congestion-ranking/. According to the press release, "[d]irect costs relate to the value of fuel and time wasted, and indirect costs refer to freight and business fees from company vehicles idling in traffic, which are passed on to households through higher prices."

[13] INRIX and the Texas A&M Transportation Institute (TTI)*, 2015 Urban Mobility Scorecard*, Aug. 26, 2015, *available at:* https://static.tti.tamu.edu/tti.tamu.edu/documents/mobility-scorecard-2015.pdf.

[14] Remarks of NHTSA Acting Executive Director Terry T. Shelton at *FTC/NHTSA Workshop.*

[15] ITS America, *The Road Ahead: The Next Generation of Mobility Public Policy Roadmap at 1*, Feb. 2017, *available at:* http://itsamerica.org/wp-content/uploads/2017/02/Final-The-Road-Ahead-The-Next-Generation-of-Mobility-Roadmap-020717b.pdf. ("*ITS America Public Policy Roadmap").*

[16] Members of the Safety Spectrum Coalition include: AAA, American Highway Users Alliance, American Traffic Safety Services Association, American Trucking Associations Association of Global Automakers, Commercial Vehicle Training Association, Intelligent Transportation Society of America, Motor & Equipment Manufacturers Association, NAFA Fleet Management Association, and National Safety Council.

[17] For example, the 5G Automotive Association has said that it "believes that ITS spectrum at 5.9 GHz will prove central to the uptake of innovative ITS solutions and business models in the years to come. Sharing of the ITS band should be approached with extreme care." 5GAA, *The Case for Cellular V2X for Safety and Cooperative Driving*, Nov. 23, 2016, *available at:* http://www.5gaa.org/pdfs/5GAA-whitepaper-23-Nov-2016.pdf.

Last year, NHTSA issued a proposed federal motor vehicle standard for V2V communications that would advance the deployment of connected vehicle technologies for cars and light trucks.[18] ITS America views the proposed V2V standard as an extremely important step forward toward ensuring the full potential of connected vehicle technology to dramatically reduce roadway fatalities, ease congestion, and transform mobility in our nation.[19]

Auto safety technologies of the past focused on crashworthiness of vehicles--protecting the driver after a crash. New technology has evolved to the point where crashes can be prevented in the first place. Industry and academic research concluded that V2V safety applications are effective and that DSRC is the most practical approach for "cooperative" crash avoidance. According to NHTSA, “safety applications enabled by V2V and V2I could eliminate or mitigate the severity of up to 80 percent of non-impaired crashes, including crashes at intersections or while changing lanes”--helping to prevent many thousands of deaths and injuries on our roads every year.[20] According to the U.S. Department of Transportation, this technology will prevent between 421,901 and 594,569 crashes by 2051 and reduce the costs from motor vehicle crashes by $53 billion to $71 billion.[21] As driverless cars begin to be deployed on our roads, V2V and V2I will expand crash avoidance capabilities, and grow industry experience and public confidence in these incredible new technologies.

V2X will allow next-generation traffic management systems that can not just report when and where congestion occurs but can adaptively direct traffic to mitigate congestion. Mobile phones and GPS will include DSRC technology that will expand V2X features into older existing vehicles, and even to protect vulnerable road users such as cyclists and pedestrians. Furthermore, most experts agree that in the long term, there will be a fundamental need for next generation automated vehicles to talk to each other and other road users.

II. DSRC Use of Data is Limited to Safety, Traffic Management, and Other Intelligent Transportation Service Applications

As defined under the Federal Communications Commission’s (FCC) technical service rules, “DSRCs systems use radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments.”[22] It is worth noting that “commercial use” of DSRC spectrum for the provision

[18] NHTSA, *Federal Motor Vehicle Safety Standards; V2V Communications*, Notice of Proposed Rulemaking, published in 82 Fed. Reg. 3854, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2017-01-12/pdf/2016-31059.pdf.

[19] ITS America Fact Sheet – Vehicle-to-Vehicle (V2V) Communications Notice of Proposed Rulemaking http://connectedvehicle.itsa.wikispaces.net/file/view/ITS+America+Fact+Sheet+White+House+Review+of+V2V+Rulemaking+April+2016+for+Docket.pdf

[20] NHTSA, *U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashe*s, Dec. 13, 2016, *available at:* *https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands*.

[21] 82 Fed. Reg. 3854, 3858.

[22] 47 CFR §90.371

of telecommunications services is not permitted by Section 90.373 of the FCC's Rules. However, like most Part 90 spectrum, DSRC spectrum may be licensed to commercial entities for the provision of DSRC services.

DSRC-enabled devices permit secure and fast short-range (approximately 300 meters) messaging called a basic safety message (BSM - Society of Automotive Engineers standard SAE J2735) containing information--such as vehicle's location, speed, heading, braking status--needed for safety critical applications.[23] The BSM is updated and broadcast up to 10 times per second to surrounding vehicles and other DSRC-equipped devices.[24] Other vehicles vehicles or devices equipped with V2X devices receive and process this information to determine collision threats.[25] If warranted, a warning could be issued to the DSRC-user to take a corrective action to avoid the collision.[26] Other SAE J2735 DSRC Message standards such as Traveler Information Message (TIM) and Signal Phase and Timing (SPAT) messages are transmitted from traffic signals and other roadside systems to vehicles to smooth traffic flow. Reducing speed variability improves traffic flow and in some cases can reduce the incidence of non-injury/non-fatality "fender bender"-type crashes which are responsible for a large portion of traffic congestion experienced on roads today.

III. Security of Intelligent Transportation Systems

Cybersecurity must be sufficiently addressed before new transportation technologies can be deployed. Cybersecurity is an enormous and complex challenge and the discussion in the June *FTC/NHTSA Connected Cars Workshop* reflected that. Improvements in techniques for designing hardware or developing software have struggled to keep up with the explosive increase in the number and complexity of critical features in nearly all domains of technology. Security authentication, access and perimeter controls must cover a larger and larger number of functions with successive generations of systems and applications. ITS America agrees with NHTSA's recommendation in their 2016 *Cybersecurity Best Practices for Modern Vehicles*[27] that a layered approach is key to reducing significantly the probability of successful automotive cyberattacks.

Layered "defense-in-depth" approach requires maintaining security controls and reacting to threats, but especially requires long term investment in secure systems design (security-by-design) by industry, which ITS America promotes through its Cybersecurity Task Force.[28] From an operational perspective, efforts are already on the way. In 2015, automobile manufacturers established an Automotive Information Sharing and Analysis Center (Auto-ISAC) to facilitate the exchange of important cyber threat information and countermeasures in real-time. Similar efforts must be made to address the security of

[23] NHTSA, V2V Fact Sheet, Dec. 13, 2016, *available at:* https://www.safercar.gov/v2v/pdf/V2V_NPRM_Fact_Sheet_121316_v1.pdf. *("V2V Fact Sheet").*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] National Highway Traffic Safety Administration. (2016, October). *Cybersecurity best practices for modern vehicles*. (Report No. DOT HS 812 333). Washington, DC.
[28] ITS America, *ITS America and Cyber Future Foundation Form Intelligent Transportation Cyber Security Task Force, May 31, 2017, available at:* http://itsamerica.org/its-america-and-cyber-future/.

traffic management systems, and ITS America is working with the Federal Highway Administration (FHWA), the American Association of State Highway Officials (AASHTO), the Institute of Traffic Engineers (ITE) and the National Electrical Manufacturers Association (NEMA) to address the security of traffic management systems. ITS America's issued a report *Cybersecurity and Dependable Transportation,*[29] that addresses how the security landscape has changed and risk management efforts may need to shift as vehicle, mobile and aftermarket devices, and traffic control systems become more and more connected and ITS applications more data-driven.

The resilience of transportation systems in the face of disruption or attack is not per se achieved through the implementation of specific technical products or services, but is emergent from a combination of design, developmental and operational security efforts. ("Emergence" means that when simple things combine to a certain degree, new properties, patterns, and behaviors develop that often cannot be explained or understood in the context of their components). Relying only on technical approaches, which may not stand the test of time, or forgetting good management policy and governance (e.g. reverting to decentralized risk management functions that produce a narrow assessment of vulnerability and risk) should be avoided.

Good guidance and best practices are essential to instilling security into technology, operations and organizations, and more and more of it is available. SAE's standard J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Standards" was released in 2016. "The National Institute of Technology and Standards (NIST) released a Framework for Improving Critical Infrastructure Cybersecurity 2014 with a new draft update for 2017.[30] Another effort is Carnegie Mellon/Computer Emergency Readiness Team (CERT) Resilience Management Model (RMM), released in 2010. A derivative of RMM is the US Department of Homeland Security's (DHS) 2016 Cyber Resilience Review (CRR), which is tailored to the needs of critical infrastructure owners and operators.[31] Institutionalization of holistic governance and risk management models/process improvement systems and standards are vital to deployment of intelligent transportation technologies whether they be in vehicles or infrastructure.

IV. Privacy of Intelligent Transportation Systems

As part of the ITS America's public policy roadmap call to remove roadblocks hindering the deployment of Intelligent Transportation, we have identified the need to build public confidence in the privacy, security, and safety of new transportation technologies.[32] ITS America, therefore, strongly agrees with NHTSA Acting Executive Director Shelton's statement at the Workshop that "[p]rivacy is...an important aspect of public acceptance of many advanced safety technologies and for these technologies to advance safety, we need public acceptance."[33] Educating consumers on how their data

[29] Cybersecurity and Dependable Transportation System, Steven H. Bayless, Sean Murphy, Anthony Shaw, ITS America, 2013 *available at* http://itsamerica.org/cyber-security-and-risk-management-in-transportation/

[30] NIST Releases Update to Cybersecurity Framework January 10, 2017 - https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework

[31] DHS CERT Cyber Resilience Review (CRR) *available at* https://www.us-cert.gov/ccubedvp/assessments

[32] *ITS America Public Policy Roadmap* at 9.

[33] Remarks of NHTSA Acting Executive Director Terry T. Shelton at *FTC/NHTSA Workshop.*

will be utilized lessens the chance speculative privacy fears will hinder the wide adoption of these technologies and the resulting safety benefits.

The ITS America policy roadmap calls for expanded support at the State and Local levels to address privacy of infrastructure technology solutions, and encourage industry and public sector to establish policies.[34] For example, in 2014, the Alliance of Automobile Manufacturers and Global Automakers issued a series of FTC-enforceable Privacy Principles regarding the offering of innovative vehicle technologies and services. Participating automakers agree to inform consumers about ways that data generated by the vehicle or driver are collected and used. The Principles treat sensitive information, such as geolocation, driver behavior, and biometric information, with additional, heightened protections.[35] ITS America also supports the work required to implement existing architecture and standards for ensuring anonymity for V2X communications using DSRC as well as, any needed engagement, with the NHTSA, FTC, and FCC. As technology evolves, privacy protection R&D must be supported.[36]

ITS America believes that a Federal standard for V2V will be key to ensuring interoperability, privacy and security, and that those standards will help support modernization of our traffic control systems through V2I communication that can improve traffic flow and reduce crashes in our most congested areas and problematic rural, suburban and urban corridors. ITS America agrees with NHTSA's assessment that DSRC-enabled V2V communications systems already contain robust privacy protections and do not collect personally identifiable information (PII). As NHTSA explains:

> By design, the V2V system will not collect, broadcast, or share information linked or linkable, as a practical matter, to individuals or their vehicles. V2V-enabled vehicles exchange only generic safety information. The system is designed to operate without using any personal information about specific vehicles or drivers.[37]

Additionally, ITS America agrees with CTIA--The Wireless Association that the Commission and NHTSA should engage with the Federal Highway Administration and corresponding state and local transportation authorities to promote the use of V2I by highlighting the technology's efficiency benefits and security protections.[38]

V. Conclusion

ITS America would like to thank the Commission and NHTSA for holding a workshop on this important topic and appreciates the opportunity to submit comments. If you have any questions or for

[34] *ITS America Public Policy Roadmap* at 9.

[35] See Comments of Auto Alliance (filed Apr. 25, 2017), *available at:* https://www.ftc.gov/system/files/documents/public_comments/2017/04/00024-140567.pdf, *and Comments of* Global Automakers (filed May 1, 2017), *available at:* https://www.ftc.gov/system/files/documents/public_comments/2017/05/00041-140624.pdf.

[36] *ITS America Public Policy Roadmap* at 11.

[37] *V2V Fact Sheet.*

[38] *See also* Comments of CTIA--The Wireless Association at 4 (filed May 1, 2017), *available at:* https://www.ftc.gov/policy/public-comments/2017/05/01/comment-00039. .

more information, please contact Steven H. Bayless, ITS America Vice President of Regulatory Affairs and Public Policy, at 202-721-4229 or via email at sbayless@itsa.org, or Jason D. Goldman, ITS America Vice President of External Affairs and Stakeholder Engagement, at 202-721-4212 or via email at jgoldman@itsa.org.

Respectfully Submitted,

/s/ Steven H. Bayless
Steven H. Bayless
Vice President, Regulatory Affairs and Public Policy
Intelligent Transportation Society of America

/s/ Jason D. Goldman
Jason D. Goldman, Esq., CIPP/US
Vice President, External Affairs and Stakeholder Engagement
Intelligent Transportation Society of America