



May 1, 2017

BY ELECTRONIC SUBMISSION

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex A)
Washington, DC 20024

Re: *Connected Cars Workshop (P175403)*

Dear FTC and NHTSA Staff:

CTIA¹ respectfully submits these comments in response to the Federal Trade Commission's ("FTC") and National Highway Traffic Safety Administration's ("NHTSA") (collectively, the "Agencies") invitation to address consumer privacy and security issues posed by connected and autonomous vehicles (the "Notice"),² in advance of the Agencies' proposed June 28, 2017 public workshop.

I. INTRODUCTION

The wireless industry, including wireless carriers, device manufacturers, and application developers, has helped create significant and widely beneficial changes in society, allowing for increased connectivity, productivity and the spread of information. Its members are actively involved in the connected

¹ CTIA-The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to live a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

² "FTC and NHTSA Seek Input on Benefits and Privacy and Security issues Associated with Current and Future Motor Vehicles" 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 (March 20, 2017).



vehicle ecosystem and the development and implementation of emerging automotive technologies, and providing connectivity technologies that make driving safer and more efficient.

As the Agencies recognize, connected vehicles can provide valuable benefits to consumers and will “revolutionize motor vehicle safety.”³ As the expert agency on vehicle safety, NHTSA has recognized the potential safety, efficiency and convenience benefits of vehicle function connectivity and automation, and has noted that regulation of advanced technologies should avoid adversely impacting the safety benefits that these technologies provide.⁴

Wireless carriers have invested heavily to ensure that reliability, security, and privacy are built into all layers of their commercial wireless network capabilities. Since 2010, wireless providers have spent \$150 billion in network improvements to deliver 4G LTE mobile broadband nationwide to U.S. consumers, making the U.S. the world leader in 4G LTE deployment.⁵ According to one recent study by Accenture, wireless operators will invest a projected \$275 billion over the next decade to deploy real-time, faster, and higher capacity 5G technology that will unlock smart communities, promote better management of vehicle traffic, and support wireless-operated self-driving cars that could save up to 21,700 lives.⁶

This level of investment is directed in large part to ensuring that wireless networks can support connected car communications such as vehicle-to-vehicle (“V2V”) and vehicle-to-infrastructure (“V2I”) reliably, safely and securely. Indeed, wireless carriers, device manufacturers and app providers ensure that privacy and security are central elements of wireless service. These industry stakeholders are working to evolve security methods addressing a broad variety of Internet of

³ Notice at 1.

⁴ NHTSA, Report to Congress: Electronic Systems Performance in Passenger Motor Vehicles at 43 (Dec. 2015), available at: http://www.nhtsa.gov/staticfiles/laws_regs/pdf/Electronic-Systems-Performance-in-Motor%20Vehicles.pdf (the “Vehicle Electronics Report”).

⁵ *The Next Generation of Wireless: 5G Leadership in the U.S.* CTIA at 3 (Feb. 9, 2016) (5G White Paper), available at: http://www.ctia.org/docs/default-source/default-document-library/5g_white-paper_web2.pdf.

⁶ See *How 5G Can Help Municipalities Become Vibrant Smart Cities*, Accenture Strategy at 1-2, 8 (Jan. 12, 2017), available at: <https://www.ctia.org/docs/default-source/default-document-library/how-5g-can-help-municipalities-become-vibrant-smart-cities-accenture.pdf> (the “Accenture Smart Cities Report”). See also *Wireless Connectivity Fuels Industry Growth and Innovation in Energy, Health, Public Safety, and Transportation*, Deloitte at 11 (Jan. 2017) available at: http://www.ctia.org/docs/default-source/default-document-library/deloitte_20170119.pdf.



Things (“IoT”) use cases, including connected transportation. Given the investment in and prioritization of privacy and data security in the wireless industry and the automotive sector, the Agencies should avoid any sector-specific regulation that would inhibit continued industry innovation and could conflict with other regulatory regimes. Instead, the Agencies should focus on establishing a national framework of technologically neutral public policies that rely on the Agencies’ respective areas of expertise and authority.

II. DATA WILL ENABLE THE SAFETY, ACCESSIBILITY AND EFFICIENCY BENEFITS OF CONNECTED AND AUTONOMOUS VEHICLES.

Vehicle data will provide consumers significant automotive safety and related societal benefits. Primary among the uses of such data is to enhance safety and crash avoidance by providing actionable information about the vehicle and its immediate surroundings, and to enabling response times and situational awareness beyond that of the typical human driver. In NHTSA rulemakings and elsewhere, CTIA supports the premise that connected vehicle technologies, combined with smart transportation infrastructure, will make U.S. roadways safer and more efficient. 5G wireless broadband networks will provide a key communications platform for these improvements.

5G network speed, capacity and location will be particularly well-suited to vehicle applications. 5G speeds will result in a 10x increase over existing 4G wireless broadband network speeds.⁷ This means that, operating on a 5G network, a self-driving, autonomous car travelling at roughly 60 mph will move *just over 1 inch* (versus 4.6 feet under the same conditions operating on a 4G LTE network) to execute a braking command once an obstacle is detected through V2V or V2I communications.⁸ 5G will also improve vehicle efficiency. The Accenture Smart Cities Report details how vehicle convoys using 5G to communicate road conditions can reduce drag, and stop-and-start driving, by 20-60%, resulting in a 25% fuel savings.⁹ Thus, 5G will enhance vehicle safety and efficiency capabilities and, “with its device density and real-time capabilities,

⁷ CTIA Comments on NTIA’s paper, *Fostering the Advancement of the Internet of Things* (the “NTIA Green Paper”) (March 13, 2017) at 2, available at: https://www.ntia.doc.gov/files/ntia/publications/ctia_comments_ntia_ietf_green_paper_3.13.17.pdf

⁸See 5G White Paper at 10-11.

⁹ See Accenture Smart Cities Report at 8.



has the potential to advance V2V features."¹⁰ Since wireless carriers will build 5G infrastructure close to roads, particularly with small cell sites and fiber connectivity, it will be readily available to support V2V and V2I communications at low latency, especially in high-density areas with great demands for data throughput from large numbers of users.¹¹

Autonomous vehicles ("AV"s) will use data to analyze road conditions and complete the driving task safely and efficiently. By relying on sensors, detailed mapping and consumer interfaces, AVs will reduce and eventually eliminate the need for a human driver. AVs will increase mobility options for consumers, regardless of their age or driving ability, increasing independence and quality of life for the elderly and disabled while promoting the safety of vehicle occupants and pedestrians.

Finally, enhanced vehicle data collection will increase vehicle reliability, avoid breakdowns, and improve overall transportation efficiency. Standardized telematics will monitor and alert drivers of maintenance issues before they occur. Over-the-air software updates will provide a more efficient and effective method of addressing these issues. Moreover, state and local transportation authorities will use V2I data through traffic light sensors and other infrastructure to manage congestion through adjusted public transportation routes and scheduling, adjusted traffic light cycles during peak and off-peak periods, and other measures. To encourage state and local government access to V2I data, the Agencies should also engage the Federal Highway Administration and corresponding state and local transportation authorities to promote efficiency benefits and security protections of connected vehicle data collected at governmental infrastructure access points. This is particularly important because such governmental use of V2I data appears to be outside the current scope of FTC or NHTSA regulatory authority.

The Notice predicts that connected vehicles are likely to collect vast amounts of data. Working with its automotive partners, CTIA members and other industry

¹⁰ *Id.*

¹¹ Still, the evolution to 5G networks, and indeed all V2X deployments that require communications to/from fixed locations, depend on timely and efficient access to wireless infrastructure, particularly for "small cell" sites that are placed on existing structures such as streetlight and utility poles. Comments of CTIA, *Streamlining Deployment of Small Cell Infrastructure by Improving Wireless Facilities Siting Policies*, FCC WT Docket No. 16-42, at 9-10 (March 8, 2017).



stakeholders have developed frameworks to protect the privacy and security of connected vehicle data.

III. THE WIRELESS SECTOR ADDRESSES DATA PRIVACY AND SECURITY INVOLVING CONNECTED VEHICLE DATA, AS IT DOES ACROSS THE INTERNET OF THINGS.

As the Notice recognizes, security issues surrounding connected vehicles are similar to those issues raised in other “connected computing platforms.”¹² For the wireless industry, network, device and mobile application privacy and data security are longstanding areas of focus. Wireless networks benefit from the security architectures standards organizations, including the 3rd Generation Partnership Project (“3GPP”), the Alliance for Telecommunications Industry Solutions, the Institute of Electrical and Electronics Engineers (“IEEE”) and the Internet Engineering Task Force.¹³ The relevant works of these organizations include 3GPP standards for over-the-air encryption and IEEE 802.11i, implemented as WPA2, and FIPS-14-2 for encryption, authentication and key management.¹⁴ Through CTIA’s Cybersecurity Working Group and other industry touchpoints, the entire mobile industry ecosystem engages in ongoing research and dialogue according to the National Institutes of Standards and Technology (“NIST”) Cybersecurity Framework to address cybersecurity threats collectively and with impacted industries.¹⁵

Establishing consumer trust and confidence in connected vehicle data use and sharing will require clear, comprehensive and consistent policies. The wireless industry takes consumer privacy seriously, offering clear, easily understood policies describing how it protects consumer data, and the choices consumers can make about how entities use or share their data.

¹² Notice at 1.

¹³ For additional discussion of relevant wireless industry security architectures, see “Protecting America’s Wireless Networks” at 4-5, available at: <http://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf> (April 2017) (the “CTIA Cybersecurity White Paper”).

¹⁴ See CTIA, “Today’s Mobile Cybersecurity – Blueprint for the Future” at 8, available at: <http://www.ctia.org/industry-data/press-releases-details/press-releases/u-s-wireless-industry-maps-its-blueprint-for-tomorrow-s-mobile-cybersecurity>) (Feb. 12, 2013).

¹⁵ See CTIA Cybersecurity White Paper at 9.



As the wireless industry has provided greater wireless connectivity and mobile devices that can integrate with motor vehicles to promote safety, CTIA and its members work closely with the automotive industry in developing privacy principles governing consumer data. In 2014, the Alliance of Automotive Manufacturers ("Auto Alliance") and the Association of Global Automakers ("Global Automakers") established Consumer Privacy Protection Principles (the "Auto Industry Privacy Principles") addressing data retrieved from vehicles.¹⁶ The Auto Industry Privacy Principles include such principles as notice and choice, transparency, respect for context, and data de-identification and security to protect data against unauthorized access or use.¹⁷ The Auto Privacy Principles are consistent with the wireless industry's own long-established principles for consumer privacy protection, and apply to new vehicles manufactured beginning in the current 2017 model year, and for vehicle technologies and services subscriptions begun or renewed after January 2, 2016.

The communications sector, which includes the wireless industry, was one of the first industry segments in 2005 to establish an industry Information Sharing & Assurance Center ("ISAC") through the Communications Sector Coordinating Council ("CSCC"). The major automobile manufacturers, led by the Auto Alliance and Global Automakers and with NHTSA's encouragement, developed and launched the automotive industry ISAC (the "Auto ISAC") in September 2015 to enable and promote the exchange of significant threat information, and countermeasures, in real time.¹⁸ NHTSA has concluded that it is "beneficial" to have an "automotive sector specific information sharing forum," and reported to Congress that the Auto ISAC "could advance the cybersecurity awareness and countermeasure development effectiveness among public and private stakeholders."¹⁹ The CSCC and Auto ISAC collaborate on cross-sector threats and responses by cybersecurity information sharing activities such as the NIST Cybersecurity Framework, through the participation of various CTIA members as

¹⁶ See, November 12, 2014 joint letter of Auto Alliance and Global Automakers to FTC Chairwoman Edith Ramirez re: "Consumer Privacy Protection Principles for Vehicle Technologies and Services," available at: <http://www.autoalliance.org/auto-issues/automotive-privacy/letter-to-the-ftc>

¹⁷ See Auto Alliance Privacy Principles for Vehicle Technologies and Services, available at: <http://www.autoalliance.org/auto-issues/automotive-privacy/principles>

¹⁸ Vehicle Electronics Report at 18; see also *Cybersecurity -- An industry-wide effort to identify emerging threats and potential adversaries*, available at: <http://www.autoalliance.org/auto-issues/cybersecurity> .

¹⁹ Vehicle Electronics Report at 17.



members of CSCC and/or Auto ISAC. The Auto ISAC's ranks have expanded comprehensively to include a broad swath of automotive component suppliers.²⁰ Wireless carriers, device manufacturers and software providers coordinate within and across sectors to detect, mitigate and respond to continually evolving security threats. Finally, CTIA is preparing an assessment of managed and unmanaged IoT network environments against industry best practices and standards. Our Cybersecurity Working Group will analyze a global model for the Internet of Things, including the transportation sector, while looking to advance cybersecurity for the U.S., and in coordination with other sectors.

The privacy and data security protections described here will apply across the CTIA membership's provision of service to the connected car ecosystem. As such, the Agencies should refrain from prescriptive regulation of wireless networks or devices, instead continuing their leadership in enforcement-based consumer protection (FTC) and vehicle safety policy (NHTSA).

IV. CONNECTED CAR DATA POLICY SHOULD BE TECHNOLOGICALLY NEUTRAL, INDUSTRY-LED, AND NATIONALLY CONSISTENT.

Our networks, devices and software operate not only in vehicles, but across the Internet of Things. Imposing any vehicle-specific privacy or security regulations could be redundant to or conflict with existing privacy and data security protections enforced by the FTC and the Department of Homeland Security ("DHS"). For example, according to a 2016 GAO Report, it remains "unclear" whether NHTSA or DHS would be "the responsible agency" for a U.S. Government

²⁰ Many suppliers of "connected car" components are recognizing the importance and value of information-sharing about vulnerabilities. At least 25 such suppliers have recently joined the Auto ISAC, furnishing additional data into its collaborative approach to cybersecurity system. Because specifications for the automotive industry are created years ahead of actual vehicle production and vehicles are becoming more and more complex, fixes can require massive and expensive recalls. That reality creates ample incentives for information-sharing and cooperation through the Auto ISAC among automotive manufacturers and suppliers by sharing threat information, including information received from U.S. government agencies. "Behind Booz Allen's effort to get carmakers to work together against hackers", Washington Post, Capital Business (March 19, 2017), available at: https://www.washingtonpost.com/business/capitalbusiness/behind-booz-allens-effort-to-get-carmakers-to-work-together-against-hackers/2017/03/19/a4e9a146-0b4f-11e7-b77c-0047d15a24e0_story.html?utm_term=.1cf7b779e595.



response to a “large-scale vehicle cyberattack on safety critical systems.”²¹ Because of the “highly-dynamic nature of cybersecurity risks and threats,” NHTSA has observed that performance standards or mandates for automotive cybersecurity are “difficult to set without the risk of becoming outdated quickly.”²²

Instead, the Agencies should continue to promote and encourage expansion of industry-led initiatives like the NIST Cybersecurity Framework and industry self-regulatory principles such as the Auto Industry Privacy Principles. Additionally, the Agencies should continue expanding understanding of privacy and security best practices through workshops, such as this one, and issuance of best practices guidance. The combination of existing self-regulating principles, NHTSA motor vehicle safety rules, and robust information sharing among automotive industry members and communications providers, will ensure that connected vehicle data is protected as its use proliferates.

Finally, federal agencies’ policies should apply consistently across state lines with expert agencies in charge of issues so that FTC policies address privacy, the NIST Framework addresses cybersecurity, and NHTSA standards address vehicle safety. State and local policymakers should commit to maximizing the societal benefit of connected vehicle data while protecting citizens’ privacy when it uses such data. With respect to the original “mobile device” (i.e., the car), consumers should be able to rely on a national framework of connected car data privacy and cybersecurity protection.

²¹ “VEHICLE CYBERSECURITY – DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack,” U.S. Government Accountability Office, Report to Congress (March 2016)(published on April 25, 2016) (“2016 GAO Report”) at 42.

²² Vehicle Electronics Report at 47.



FTC/NHTSA Connected Cars Workshop
May 1, 2017
Page 9

Respectfully submitted,

CTIA

By: /s/ Maria Kirby
Maria Kirby
Assistant Vice President, Regulatory Affairs

/s/ Jackie McCarthy
Jackie McCarthy
Assistant Vice President, Regulatory Affairs