

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of)
Connected Cars Workshop) Project No. P275403
)
)
)

**COMMENTS OF THE CONSUMER TECHNOLOGY
ASSOCIATION**

I. INTRODUCTION AND SUMMARY

The Consumer Technology Association (“CTA”)¹ is pleased to submit these comments in anticipation of the workshop on the benefits and privacy and security issues associated with connected and automated vehicles hosted by the Federal Trade Commission (“FTC”) and the National Highway Traffic Safety Administration (“NHTSA”). CTA works to advance public policy that fosters innovation, furthers economic competitiveness, and promotes job and business creation. Our members are engaged in every aspect of technology and innovation, including traditional consumer technology companies, sharing economy and internet companies, and auto manufacturers and suppliers. CTA’s members are bringing life-changing developments to the auto industry that will offer consumers greater convenience, cutting-edge advances in vehicle functions and, most importantly, improved safety.

¹ The Consumer Technology Association (CTA)TM is the trade association representing the \$292 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world’s best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world’s gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA’s industry services.

As vehicles become increasingly connected, addressing concerns and providing education about security and privacy is very important. In the public notice for the upcoming workshop, the FTC and NHTSA have highlighted some of the key issues of data, privacy, and cybersecurity associated with connected and automated cars. These issues merit focus from all stakeholders. Indeed, industry stakeholders already are proactively addressing them – but it is critical to consider privacy and cybersecurity alongside the life-changing and life-saving benefits of connected and automated vehicles can and will bring, as the FTC has recognized since it examined connected cars as part of its Internet of Things workshop and report.²

While considering the myriad benefits, the U.S. government should approach the connected and autonomous car landscape through flexible, predictable, and innovation-friendly policies. CTA encourages the FTC and NHTSA to explore ways that the U.S. government and other stakeholders can help to unleash the benefits of this next generation of automobiles. Avoiding inconsistent and prescriptive regulation is critical in this regard. However, certain proactive steps by FTC and NHTSA, such as working with federal and state government partners to develop a consistent approach toward connected and automated vehicle privacy and security, could aid the development and deployment of these new, next generation automotive technologies.

² See FTC, *Internet of Things: Privacy and Security in a Connected World* 9 (2015), available at <https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices> (“On the road, connected cars will increasingly offer many safety and convenience benefits to consumers.”).

I. DISTINCTION BETWEEN CONNECTED AND AUTOMATED VEHICLE TECHNOLOGIES

At the outset it is critical to appreciate the distinction between connected and automated vehicles. The differences between connected and automated vehicle technologies have direct implications for security and privacy. Therefore, they should not be conflated.

Connected vehicles are equipped with a *wireless connection* via a built-in or device-enabled radio. Eventually, connected cars may use these wireless connections to “speak” with one another (V2V) and road-side infrastructure (V2I). Automated vehicles, by contrast, do not rely on a wireless connection. Automated vehicles utilize vehicle-resident technologies like sensors, maps, LIDAR, HD cameras, and GPS to navigate and “drive” without human interaction. While connected vehicle technologies (*i.e.*, wireless connections) may ultimately serve as a second source of data for automated vehicles, automated vehicles can and *must* be able to operate in the absence of network connectivity. Automated vehicles’ dependence on vehicle-resident technologies is critical to their functional safety.

This distinction between connected (wireless technologies) and automated (vehicle-resident technologies) becomes particularly important when discussing the security and privacy of vehicle data, as the preponderance of risk arises from connectivity, *i.e.*, the two-way transmission of data to and from the vehicle. Thus, when discussing vehicle security and privacy policy, it is critical to not conflate connected and automated vehicles, but rather to appropriately focus on wireless connectivity and connected vehicle technologies.

II. THE CONNECTED AND AUTOMATED CAR REVOLUTION WILL PROVIDE TREMENDOUS BENEFITS TO THE U.S. ECONOMY AND CONSUMERS

The connected and automated car revolution will provide immense economic and societal benefits to the U.S. economy and consumers, and their promise became even more evident at this year's CES.³ Car technology on display at CES 2017 included:

- New autonomous and semi-autonomous vehicles and concept cars from Ford, Nissan, and others, including an autonomous concept car that will take over for fatigued drivers and provide greater independence and mobility to individuals with disabilities;
- A fully autonomous vehicle developed by Mercedes that carries and deploys drones for front-door autonomous delivery; and
- Cross-company technology integration, including Ford's incorporation of Amazon's cloud-based virtual assistant, Alexa, in select vehicles, enabling drivers to control devices in their homes (*e.g.*, set a thermostat) from their cars and control some aspects of their cars (*e.g.*, starting their engines or locking their doors) remotely.⁴

There are many other examples of vehicle innovations and benefits across the industry. For example, in a significant step towards the introduction of BMW's first fully autonomous vehicle in 2021, BMW, Intel and Mobileye are collaborating this year to globally test a fleet of 40 automated vehicles under real-world traffic conditions that will perform with consistent, predictable behavior and are validated to the highest level of safety – enabling a wide range of new and differentiated consumer experiences.⁵

³ See, *e.g.*, Samara Lynn, *CES 2017 Was All About Incredibly Smart Cars*, Black Enterprise, Jan. 10, 2017, <http://www.blackenterprise.com/technology/ces-2017-incredibly-smart-cars/> (“If there was one, star attraction at CES this year, arguably it was vehicles.”).

⁴ See Cadie Thompson, *All the most important car tech that came out of CES 2017*, Business Insider, Jan. 9, 2017, <http://www.businessinsider.com/ces-2017-car-tech-concept-cars-2017-1/#ford-debuted-its-new-autonomous-test-vehicle-1>.

⁵ Intel, *BMW Group, Intel and Mobileye Will Have Autonomous Test Vehicles on the Roads by the Second Half of 2017* (Jan. 4, 2017), <https://newsroom.intel.com/news-releases/bmw-group-intel-mobileye-will-autonomous-test-vehicles-roads-second-half-2017/>.

Until very recently, the automotive technology on display at this year's CES lived only in Hollywood science fiction scripts. Once deployed, these innovations will transform countless aspects of consumers' lives and the U.S. economy in the ways described below, and many others.

Next-generation cars will save thousands of lives each year. As NHTSA fully knows, human error leads to a staggering number of vehicle-related deaths. More than 30,000 people die on U.S. roads each year, and a staggering 94 percent of these deaths are tied to at least some element of human choice and human error.⁶ Advances in connected car technology – including crash avoidance technologies – will help to make our roads far safer than they are today.

Smarter cars will help build smarter cities and save Americans' time. Automated vehicles, connected vehicles, and connected infrastructure will help city planners build smarter cities and transportation systems, potentially resulting in less traffic congestion and reducing the many costs associated with it. For example, if autonomous car-sharing is fully embraced, as many as seven of eight cars may no longer need to be on the road, reducing both traffic congestion and the need for parking spaces.⁷ Autonomous vehicles may also transform the experience of riding in a car by allowing the “driver” to take his or her eyes off the road in order to work or read, thus making time spent in a car more productive and enjoyable.⁸

⁶ U.S. Department of Transportation and NHTSA, *Federal Automated Vehicles Policy*, at 5, Sept. 2016 https://one.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf.

⁷ See Patrick Sisson, *How Driverless Cars Can Reshape Our Cities*, Curbed, Feb. 25, 2016, <http://www.curbed.com/2016/2/25/11114222/how-driverless-cars-can-reshape-our-cities>.

⁸ See Paul Mackie, *Two keys to how autonomous vehicles could ease congestion*, Mobility Lab, June 16, 2016, <https://mobilitylab.org/2016/06/16/two-keys-autonomous-vehicles-ease-congestion/>.

Autonomous vehicles can substantially reduce insurance costs. According to insurance broker Aon, premiums for U.S. auto insurers could drop more than 40 percent once autonomous cars are fully deployed on U.S. roads.⁹

Self-driving cars can offer newfound mobility and independence for many individuals without them now. Self-driving cars also can empower Americans with disabilities and senior individuals currently unable to drive. For instance, in December 2016, Steve Mahan, who is legally blind, became the first non-Google employee to ride alone in Google's autonomous car as he traversed the streets of Austin, Texas.¹⁰

These expected benefits – and benefits we cannot yet predict – will only accrue to consumers and the economy if the automobile and tech industries are allowed to innovate. As U.S. government agencies and other stakeholders consider the future of connected car technology, they should never forget the tremendous benefits such technology can bring can bring individuals and the economy as a whole.

III. CONSUMERS WANT THE NEXT GENERATION OF AUTOMOBILES – AND INDUSTRY KNOWS IT MUST MAINTAIN CONSUMERS' TRUST TO DELIVER THEM

Consumers are excited about driverless vehicles and the benefits they will bring. According to a CTA study, two-thirds of consumers wish to exchange their current cars for autonomous vehicles, and seven out of ten consumers are ready to give a self-driving car a test

⁹ See Oliver Suess and Jan-Henrik Foerster, *Self-Driving Cars to Cut U.S. Insurance Premiums 40%, Aon Says*, Bloomberg, Sept. 11, 2016, <https://www.bloomberg.com/news/articles/2016-09-11/self-driving-cars-to-cut-u-s-insurance-premiums-40-aon-says>.

¹⁰ See Ashley Halsey III and Michael Laris, *Blind man sets out alone in Google's driverless car*, Dec. 13, 2016, https://www.washingtonpost.com/local/trafficandcommuting/blind-man-sets-out-alone-in-googles-driverless-car/2016/12/13/f523ef42-c13d-11e6-8422-eac61c0ef74d_story.html.

drive.¹¹ Moreover, almost all drivers that currently use some sort of semi-autonomous or driver-assist technology appreciate such enhanced capabilities. For instance:

- 96 percent like or love automatic parking-assist capabilities;
- 94 percent like or love collision avoidance systems;
- 94 percent like or love car maintenance alerts; and
- 97 percent are satisfied with their navigation assistance.¹²

Connected vehicles also offer new benefits. However, advancing and improving connected and automated cars depends on the collection and sharing of information – some of which is personal – among devices. Vehicle manufacturers, as well as tech companies that are bringing new connected technologies to the automobile, understand that protecting vehicle-related data – and the devices that collect, transmit, and use the data – is integral to maintaining the trust that consumers have in their vehicles. Moreover, these companies have long understood that trust is essential to their success. Without trust, consumers will not purchase and adopt new technologies and services, no matter how great their benefits. Addressing privacy and security challenges is part of maintaining this trust.

Consequently, the industry is focused on providing appropriate privacy and security protections for personal data. For example, in November 2014, members of the automotive industry committed to follow the *Privacy Principles for Vehicle Technologies and Services* in order to address new privacy issues raised by embedding connected technology in vehicles.¹³

¹¹ See CTA Press Release, *Revved Up and Ready: Most Consumers Are Excited About Driverless Cars and Their Many Benefits, says CTA Study*, Oct. 7, 2016, <https://www.cta.tech/News/Press-Releases/2016/October/Revved-Up-and-Ready-Most-Consumers-are-Excited-A.aspx>.

¹² *Id.*

¹³ See Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc., *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and*

The principles set forth a series of enforceable requirements for participating members based on the Fair Information Practice Principles. Among other things, the principles call for affirmative consent if participating members use driver behavior information for marketing or share such information with unaffiliated third parties for their own purposes.¹⁴

The industry also has sought to proactively address cybersecurity challenges. In the summer of 2015, members of the automotive industry announced the Automotive Information Sharing and Analysis Center (“Auto-ISAC”) to share information and collaboratively address cybersecurity threats.¹⁵ The industry subsequently developed and released a framework for cybersecurity best practices, applying elements of the NIST Cybersecurity Framework,¹⁶ which, in turn, culminated in the development and release of best practices last summer.¹⁷ These best practices offer individual companies ways to enhance automotive cybersecurity within their organization, and cover the full gamut of organizational and technical aspects of cybersecurity, including governance, risk management, security by design, threat detection, incident response, training, and collaboration with appropriate third parties.¹⁸ The Auto-ISAC has committed to

Services, Nov. 12, 2014, https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.

¹⁴ *Id.* at 8.

¹⁵ Auto-ISAC, Frequently Asked Questions, <https://www.automotiveisac.com/faq.php>.

¹⁶ The NIST Cybersecurity Framework is emblematic of the sort of innovation-friendly policies that can help the U.S. unleash economic growth and maintain its global leadership role in technology, including with respect to connected and autonomous vehicles. *See generally* Comments of the Consumer Technology Association to NIST on the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (filed Apr. 10, 2017).

¹⁷ Auto-ISAC, Automotive Cybersecurity Best Practices: Executive Summary, July 2016, <https://www.automotiveisac.com/best-practices/>.

¹⁸ *See id.*

updating the best practices over time to address emerging cybersecurity areas and reflect the always evolving cyber landscape.¹⁹

These proactive industry-led efforts – in contrast to a top-down regulatory approach – will best ensure that industry meets privacy and cybersecurity challenges without unnecessary government restrictions that will inhibit industry’s ability to develop and bring to market next-generation automotive technologies.

IV. THE FTC AND NHTSA SHOULD LOOK FOR WAYS FOR THE FEDERAL GOVERNMENT TO ADVANCE, RATHER THAN INHIBIT, THE CONNECTED AND AUTOMATED CAR REVOLUTION

In light of the remarkable promise of this next phase of automotive technology, CTA encourages the FTC and NHTSA to explore the ways that different stakeholders can help to unleash the connected and automated car revolution. Avoiding overly broad and prescriptive rules to address hypothetical harms – which can harm vehicle safety innovation and inhibit security innovations that can save lives – is one way. But the agencies can also take affirmative steps to encourage innovation. For instance, a clarification of the FTC’s and NHTSA’s respective roles in this emerging ecosystem, and a commitment to ensure a consistent and predictable, innovation-friendly government approach, would help establish a regulatory environment that fosters innovation. The agencies have some history of staying in step on privacy and security issues, as is evident in the FTC’s 2014 comments praising NHTSA’s consideration of privacy and security issues in its proposed V2V communications standard.²⁰

The joint workshop presents an opportunity to further develop this collaboration.

¹⁹ *See id.*

²⁰ *See generally* Comments of the Federal Trade Commission, Docket No. NHTSA-2014-0022, (filed Oct. 20, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf.

Unfortunately, the potential for inconsistent regulatory approaches is only growing. The introduction of connected technologies in vehicles could cross traditional sector-specific regulatory silos. With this convergence in technology comes the potential for oversight to be inconsistent or duplicative across agencies. Vehicle safety issues, for example, fall squarely within NHTSA’s jurisdiction and wheelhouse, while the FTC has long been the primary privacy and data security regulator in the U.S. As cars become more connected, jurisdiction may become less clear and other federal agencies may seek to play a role – or be asked to play a role²¹ – in evolving and converging connected car issues.

Any fragmented, divergent, or inconsistent regulatory approaches could chill the development of connected cars. Different approaches to different, interrelated players and services also can be confusing to consumers and distort competition. For instance, a data privacy framework that treats navigation assistance technology that is embedded in the car’s dashboard differently from the same technology on the driver’s phone would lead to uneven protection for the same data, confuse consumers, and create an uneven playing field for competition. A coordinated federal approach is therefore important, and the FTC-NHTSA workshop could provide the first step toward ensuring that these agencies play complementary, rather than overlapping or conflicting, roles.

State laws and regulations also have the potential to fragment the connected car privacy and security regulatory landscape. The FTC can play a valuable role in monitoring state

²¹ For instance, certain advocacy organizations last year sought the intervention of the Federal Communications Commission to impose new car safety, cybersecurity, and privacy obligations on car manufacturers, despite the agency’s clear lack of authority and expertise to do so. *See* Petition for Rulemaking and Request for Emergency Stay of Operation of the Dedicated Short-Range Communication Service in the 5.850-5.9925 GHz Band (5.9 GHz Band) of Public Knowledge and the Open Technology Institute at New America, RM-11771 (filed June 28, 2016).

legislative and regulatory activity that interfere with nationally consistent standards and encouraging states to refrain from adopting measures that could lead to confusion and inconsistency across state borders.²²

V. CONCLUSION

The joint FTC-NHTSA workshop is an important step toward examining the broad range of privacy and security issues that arise from increasingly connected and automated vehicles. CTA appreciates the agencies' effort to gather input from stakeholders through this forum. CTA supports this effort and encourages the FTC and NHTSA to ensure a consistent, predictable, and innovation-friendly government approach. CTA stands ready to be a resource for the FTC and NHTSA going forward.

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION

By: /s/ Julie M. Kearney

Julie M. Kearney
Vice President, Regulatory Affairs
Jamie Boone
Senior Director, Government Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

April 28, 2017

²² For example, the FTC has pointed out that specific legislation at the state level could inhibit competition. *See, e.g.*, FTC Staff Comment on Ohio State Legislative Effort to Enhance Access to Dental Care (Mar. 9, 2017), <https://www.ftc.gov/news-events/press-releases/2017/03/ftc-staff-comment-ohio-state-legislative-effort-enhance-access>.