ctia™
Everything Wireless

March 10, 2016

The Honorable Hannah Beth Jackson
Chair, Senate Judiciary Committee
State Capitol, Room 2032
Sacramento, CA 95814

The Honorable Jim Beall
Chair, Senate Transportation and Housing Committee
State Capitol, Room 5066
Sacramento, CA 95814

RE: "Telematics 101" Informational Hearing

Dear Senators Jackson and Beall:

CTIA appreciates this opportunity to write to you in response to a series of questions about the involvement of the wireless industry in the evolving ecosystem of connected cars and the role of cybersecurity and privacy. CTIA is an international nonprofit trade association that has represented the wireless communications industry since 1984. Our members include the nation's wireless carriers, handset manufacturers, operating system developers and their suppliers. This letter is intended to highlight the role CTIA members play in the diverse and robust arena of telematics and the connected car. We hope this information is useful to Committee members.

The term 'telematics' comes from the combination of the words telecommunications and informatics. The connected car offers tremendous benefits to consumers. This area has also emerged as an exciting and innovative opportunity for CTIA's membership, as well as many other companies that participate in this ecosystem. The benefits provided today by telematics services are immense and continue to develop. Telematics enables data to be captured from vehicles and converted into useful information such as mileage, fuel efficiency, driver behavior, accident analysis and lost or stolen vehicle recovery. [1,2] Telematics can also make driving more efficient through fleet management services, infotainment, roadside assistance and traffic flow management. [3,4] In fact, it is

---

[1] "Telematics Leads to Increased Driver Safety and Substantial Savings," Global Fleet Insights, August 2015; http://www.globalfleetinsights.com/fleet-management/2015/08/telematics-leads-to-increased-driver-safety-and-substantial-savings/, last accessed 3/2/2016.

[2] For example, GM/OnStar's emergency services and automatic crash notification in particular have helped save many lives.

[3] "AT&T Will Improve Your Morning Commute," AT&T Innovation Space Blog, September 2015, http://about.att.com/innovationblog/09292015smartcities, last accessed 3/2/2016. *See also*, "GM Could Crowdsource Your Car's Data to Make Better Maps for Self-Driving Cars," The Verge, January 2016, http://www.theverge.com/2016/1/5/10714374/gm-crowdsourced-self-driving-maps-onstar-ces-2016, last accessed 3/2/2016.

estimated that 100% of cars will be connected (either by embedded, tethered or smartphone integration) in multiple ways by 2025. [5,6]

CTIA members play an integral role in this area by providing a variety of services to car companies. Original Equipment Manufacturers ("OEMs" e.g., car manufacturers) can build telematics devices into a vehicle. Consumers can also install telematics devices after market and connect using wireless technology (such as Bluetooth) or through the OBD II (On Board Diagnostics) port. A typical car has many electronic devices built in, and many are connected together using a CAN (Controller Area Network), a method to connect all the various devices together, resulting in a local network within the vehicle.

Wireless carriers support telematics services in a variety of ways. They offer the network connectivity that carries the signals from the vehicles and can also offer the telematics application servers that OEMs use to develop the services that go into the vehicle. Wireless carriers can also offer both connectivity and solutions through the sale of aftermarket devices that deliver telematics services to subscribers. Wireless carriers provide telematics services to deliver safety, communications, security and infotainment.

Privacy and Security

CTIA members represent a cross-section of the connected car ecosystem and are committed to the privacy and security of the consumer information with which they are entrusted. Our members are transparent about their practices and utilize various methods to advise consumers about how their information will be handled. In addition, our members inform consumers about the choices they have with regard to their information and are committed to honoring those choices.

With respect to privacy, wireless carriers that offer connectivity for telematics services only transmit consumer data and ordinarily do not interact with it, and as such may be involved in securing the data but do not typically enter into service contracts directly with telematics consumers. OEMs offering embedded telematics solutions or telematics services typically handle the privacy protections for the service through contracts with end-users. These contracts detail how information is collected, used and disclosed when a customer signs up for service. Data is typically transmitted from vehicles upon an event such as a call for in-vehicle information or roadside assistance. Data transmitted may be used to provide services to subscribers, such as nearby restaurant recommendations based on location received, or to dispatch roadside assistance or emergency services

---

[4] See Figure 1.
[5] "Connected Car Forecast: Global Connected Car Market to Grow Threefold Within Five Years," GSMA mAutomotive, May 2013, http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf, last accessed 3/1/2016.
[6] See Figure 2.

based on location. These contracts typically disclose how and whether data is shared with partners or third parties.

Security is just as important as privacy, because without security there can be no privacy. Security in the connected car involves the numerous ecosystem players that play a role in this area, including wireless carriers, app developers, OEMs and device manufacturers. In addition to the protections that wireless carriers put in place to secure their networks in their roles as transport providers, our members use a variety of methods to fight against the infiltration of malicious code and other unauthorized access to customer information such as authentication, secure storage, private networks, physical security and other measures. The U.S. National Institute for Standards and Technology National Cybersecurity Framework provides useful awareness of cybersecurity in all areas (discussed further below).

Federal Developments

At the federal level, there are a host of connected car policy developments worth noting. These activities focus on encouraging continued investment in telematics and the connected car and developing common security standards.

In August 2014, the Department of Transportation (DOT) issued a Vehicle-to-Vehicle (V2V) Advanced Notice of Proposed Rulemaking (ANPRM) intended to examine the technical feasibility of V2V technologies, its privacy and security and preliminary estimates on costs and safety benefits. [7] V2V technology standards development "represents the next great advance in saving lives." The National Highway Traffic Safety Administration (NHTSA) estimates that once all vehicles are equipped, V2V could potentially mitigate 80 percent of non-impaired crashes, reducing more than $800 billion in costs to our nation's economy each year.[8] The DOT notes, "V2V technology does not involve collecting or exchanging personal information or tracking drivers or their vehicles. The information sent between vehicles does not identify those vehicles, but merely contains basic safety data. In fact, the system as contemplated contains several layers of security and privacy protection to ensure that vehicles can rely on messages sent from other vehicles."[9] Furthermore, the DOT has emphasized that V2V communications must not interfere with

---

[7] "U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology," August 18th, 2014, http://www.nhtsa.gov/About+NHTSA/Press+Releases/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications, last accessed 2/28/2016.

[8] "How Autonomous Vehicles Will Shape the Future of Surface Transportation," Before the House Committee on Transportation and Infrastructure Subcommittee on Highways and Transit, November 19, 2013, 113th Cong., Washington, D.C. (statement of David L. Strickland, Administrator, National Highway Traffic Safety Administration), https://transportation.house.gov/uploadedfiles/2013-11-19-strickland.pdf, last accessed 3/9/2016.

[9] See Footnote 7.

other devices. As this rulemaking unfolds, it is important to note that state-specific regulation may prove to be impractical given that these technologies are designed to travel across state lines.

The ongoing work at the U.S. National Institute for Standards and Technology (NIST) on its National Cybersecurity Framework is another critical effort that is aiding industry in enhancing telematics and connected car data security.[10] The framework is the result of a government-convened, industry-led process to develop cybersecurity frameworks for numerous critical infrastructure sectors, including telecommunications, electricity and transportation. CTIA members are actively involved in this process, and because mobile network operators have prioritized cybersecurity since they began building wireless networks, they already have a foundational set of practices on which to build. The wireless industry has integrated all players in the mobile ecosystem – carriers, manufacturers, app developers and operating systems – into its approach to cybersecurity. As stated, this framework has applicability to the connected car/telematics space.

In December 2015, Congress passed and the president signed into law the Fixing America's Surface Transportation (FAST) Act, which included the Driver Privacy Act of 2015. The Driver Privacy Act specifies the conditions that vehicle data recorded or transmitted by an Event Data Recorder (EDR, as defined in 49 C.F.R. §563.5) may be retrieved. The conditions are as follows: (1) upon court order; (2) with the owner or lessee's written, electronic or recorded audio consent—including consent for the purpose of diagnosing, servicing, repairing the vehicle or by agreeing to a subscription service that describes how the data will be retrieved or used; (3) pursuant to an investigation under 49 U.S.C. §1131(a) or 30166 when personally identifiable information is not disclosed; (4) for the purpose of determining the need for or facilitating emergency medical response; and (5) for traffic safety research when personally identifiable information is not disclosed in connection with the retrieved data.

Further, this month in Congress, four bipartisan Senators have proposed the Developing Innovation and Growing the Internet of Things (DIGIT) Act. This act calls for a federal working group to examine four aspects of the Internet of Things: the regulatory environment, current and future connectivity needs, consumer protection—including privacy and security—and current use of technology by Federal agencies. The U.S. Department of Transportation would be a member of this working group, in recognition that connected cars, telematics and fleet and freight management are each related elements of the broader Internet of Things, and that policies addressing these must be developed in a manner that is sensitive to the broader Internet of Things context.

Finally, it is important to point out existing Federal and state laws protect the privacy and security of consumer information such as the data collected by telematics providers. For

---

[10] NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/, last accessed 2/28/2016.

example, both Federal law and similar state laws prohibit certain entities from engaging in unfair or deceptive practices. Thus, if a telematics provider misrepresented its practices or failed to reasonably protect a customer's information, such a provider could be subject to enforcement by both Federal and state agencies in the area of privacy and security.

In closing, thank you for the opportunity to highlight the exciting new developments in the automotive telematics and connected car space. CTIA's members are continuously on the forefront of this exciting technology as we seek to provide new services that enhance our consumers' experiences and security while also safeguarding their privacy.

We appreciate the Committees' interest in this area. Given the well-developed framework to protect consumers against unfair and deceptive privacy and security practices, and the fact that these technologies by their nature traverse state lines, we believe that state-by-state legislative activity is unnecessary and potentially detrimental to the developing connected car marketplace.

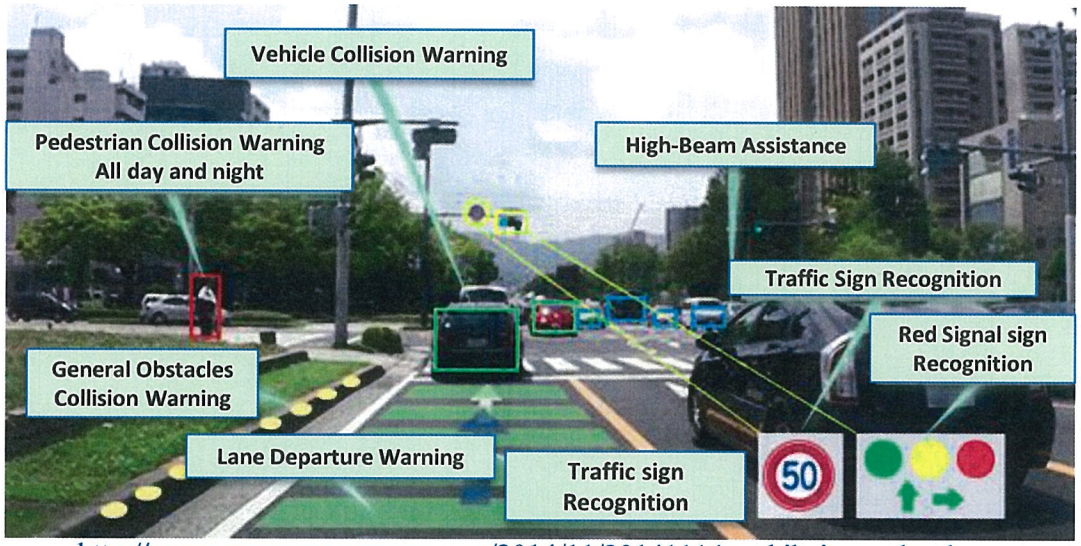
Sincerely,

Jamie Hastings
Vice President, External and State Affairs
CTIA-The Wireless Association

cc: Honorable John Moorlach, Vice Chair, Senate Judiciary Committee
Honorable Anthony Canella, Vice Chair, Senate Transportation and Housing Committee
Toby Halvarson, Consultant, Senate Judiciary Committee
Randy Chinn, Chief Consultant, Senate Transportation and Housing Committee
Mike Petersen, Senate Republican Policy Staff
Ted Morley, Senate Republican Policy Staff

Figure 1
V2X Communications

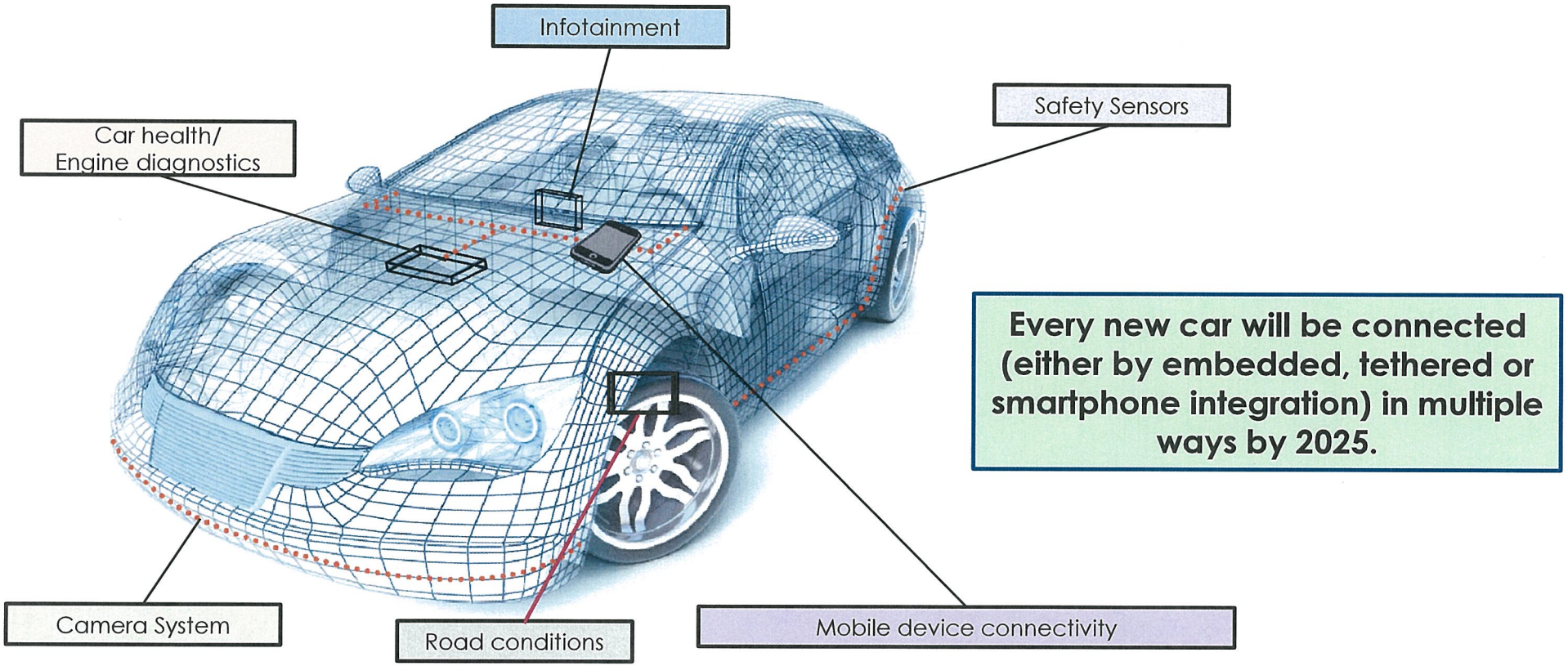
ctia™
Everything Wireless



http://www.greencarcongress.com/2014/11/20141114-toshibaimage.html

Figure 2
Connected Car

ctia™
Everything Wireless



Every new car will be connected (either by embedded, tethered or smartphone integration) in multiple ways by 2025.