U.S. House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Information Technology, and Subcommittee on Transportation and Public Assets

"Internet of Cars" Hearing
Testimony of Dean C. Garfield, President and CEO
Information Technology Industry Council
November 18, 2015

Good afternoon. Thank you Chairman Mica, Chairman Hurd, Ranking Member Duckworth, and Ranking Member Kelly, and members of the subcommittees for inviting me to testify today. The focus of this hearing – smart, autonomous, and connected vehicles – is no longer a thing of the future. The benefits that come from the convergence of the automobile and technology are already being realized; unfortunately, with new technology comes new, potential threats – threats that have been widely reported in this space. Given this backdrop, this is an important and timely hearing to discuss innovations the technology industry is making in this space, as well as to find a collaborative path forward with the Committee and Congress that ensures we maximize the potential intelligent vehicles will provide consumers, the environment, and our economy.

My name is Dean C. Garfield, and I am President and CEO of the Information Technology Industry Council (ITI). ITI represents 62[1] of the most innovative and forward-looking companies in the world. Our membership includes companies from all verticals of the technology sector, including semiconductor, network equipment, software, digital services, hardware, mobile devices, Internet companies, as well as companies that are using technology to fundamentally evolve their businesses. Going forward, every one of these verticals will be a supplier of parts, components, systems, or services to the automotive sector. Congress and the federal government will play a critical role in the development of this market, as well as in the safety and security of the American driving public.

My testimony today will focus on three areas: 1) the benefits and potential of intelligent, autonomous and connected vehicles; 2) transportation and automotive cybersecurity; and 3) recommendations for legislative priorities in the Internet of Things (IoT) and intelligent vehicle space.

[1] See membership list here: http://www.itic.org/membership/member-companies

The Promise of Intelligent Automobiles

Since the turn of the 21st century, we have seen enormous advances in technology. A combination of mobile connectivity, robust and affordable broadband, exponential advances in computing power, and unprecedented data storage and processing capabilities have changed the way technology is utilized. Taking those advances and applying them to applications that were previously not digitized has given rise to the Internet of Things. The transportation and automotive sectors are one of the most promising beneficiaries of that evolving field. With the embedding of technology throughout the automobile, we have seen improvements in performance, maintenance, reliability, and most importantly, safety and efficiency.

While these advances are present in the marketplace today, the consumer intelligent vehicle marketplace is really only in its infancy. Advanced braking assistance, adaptive cruise control, lane departure controls, left-turn assistance, blind spot detection and notification, and parking assistance are a few of the advanced driver assistance systems (ADAS) currently available and increasing in market penetration. Each of the other companies here today have incorporated some combination of these technologies into their vehicles.

The next major jump in smart vehicle capabilities that will fundamentally change the way we utilize automobiles will come from vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and autonomous vehicle capabilities. In the V2V and V2I space, there are various technologies being tested to deliver these capabilities, and ITI companies are working on each of them. Advanced Long Term Evolution (LTE-Advanced),[2] Dedicated Short Range Communication (DSRC),[3] and fifth generation (5G) wireless technology[4] are all being developed and tested for use in connected vehicle safety applications. Each of these provide specific characteristics needed to reliably enable vehicles to connect with wireless networks, transportation infrastructure, and other vehicles, and low enough latency to provide information in the matter of milliseconds necessary to make critical safety calculations and respond.

Similarly, ITI companies are working on autonomous vehicle technology and systems, some of which may be designed to rely on connected vehicle technology as well, while others are testing autonomous vehicle systems that will not rely on connected vehicle technology. The marketplace for these technologies is still developing, and should be allowed to continue to do so without a finger on the scale to determine which technology or technologies are ultimately widely adopted and deployed. ITI has submitted comments in National Highway Traffic Safety Administration's (NHTSA) rulemaking process for V2V Communications providing additional

---

[2] *Cars Talk to Cars on the Autobahn*, IEEE Spectrum, November 10, 2015, http://spectrum.ieee.org/cars-that-think/transportation/infrastructure/cars-talk-to-cars-on-the-autobahn

[3] *See* U.S. Department of Transportation, Overview of Dedicated Short Range Communication, http://www.its.dot.gov/dsrc/

[4] *How 5G Will Push a Supercharged Network to Your Phone, Home, Car,* CNet, March 2, 2015, http://www.cnet.com/news/how-5g-will-push-a-supercharged-network-to-your-phone-home-and-car/ and *The Smartest Cars May Need 5G Networks, Ericsson Says*, PCWorld, January 18, 2014, http://www.pcworld.com/article/2089440/the-smartest-cars-may-need-5g-ericsson-says.html

information about the various technologies companies are developing, and the need to refrain from mandating specific technologies.[5]

What is most exciting about all of these advances is the potential to protect human health and lives. The World Health Organization estimated that in 2010, there were 1.24 million deaths on the world's roadways,[6] and the US Census Bureau reports there were 10.8 million accidents on U.S. roadways in 2009.[7] Human error contributes to 90 percent of automobile accidents.[8] Fully realized, ADAS systems will prevent approximately 30 percent[9] of all automotive accidents, and automated vehicles can prevent up to 90 percent.[10] These are staggering numbers. Everyone one of us knows someone who has been in a serious automobile accident; potentially preventing 90 percent of accidents will take one of the largest sources of traumatic injury out of our hospitals.

Directly related to this are the economic benefits derived from the reduction in accidents. The economic costs of automobile accidents stem from property damage, lost earnings, lost household earnings, medical costs, legal costs, and many other impacts. Annual costs from injuries amount to $365 billion, and costs from fatalities amount to $260 billion.[11] If there were a 90 percent reduction in accidents, the positive economic impact would be more than half a trillion dollars, or $563 billion.[12]

Countless other benefits, both economic and societal, will be derived from autonomous and connected vehicles, including increased productivity from time not spent focusing on driving, decreased congestion, and fuel savings from less congested roadways. Similarly, a vehicle able to operate autonomously will be able to deliver a passenger to their destination, and be shared by family members or others. This provides families additional flexibility while also preventing cars from sitting unused for hours on end in city streets or parking garages. A related benefit will be the increased mobility of individuals not capable of operating a vehicle today, namely the elderly, disabled, and youth; providing much more convenient, safe, and flexible

---

[5] *See* ITI comments in NHTSA's advanced notice of proposed rulemaking Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle Communications, http://www.regulations.gov/#!documentDetail;D=NHTSA-2014-0022-0403

[6] World Health Organization, Global Health Observatory Data, Number of Road Traffic Deaths http://www.who.int/gho/road_safety/mortality/en/

[7] Statistical Abstract of the United States: 2012, U.S. Census Bureau, Section 23: Transportation, 1103 Motor Vehicle Accidents http://www.census.gov/library/publications/2011/compendia/statab/131ed/transportation.html

[8] *See* "Human error as a cause of vehicle crashes," blog entry by Bryant Walker Smith, Center for Internet and Society at Stanford Law School, December 18, 2013, http://cyberlaw.stanford.edu .

[9] *A Roadmap to Safer Driving*, Motor Equipment Manufacturers Association and the Boston Consulting Group, 2015, page 1.

[10] *Urban Mobility at a Tipping Point,* McKinsey and Company, September 2015 http://www.mckinsey.com/insights/sustainability/urban_mobility_at_a_tipping_point

[11] *Nikola's Revenge: TSLA's New Path of Disruption*, Morgan Stanley Research North America, February 25, 2014, pages 25-26.

[12] *Ibid.*.

transportation options than may currently be available to these populations. The economic impacts from this increased safety and reduction of accidents, reduced fuel consumption, and added productivity has been estimated to be more than a trillion dollars.[13] Lost time, wasted fuel, and increased cost of doing business alone cost as much as two to four percent of the national gross domestic product.[14] The future of intelligent, autonomous, and connected cars will not just solve these problems of today; it will create new opportunities we have not yet contemplated.

Securing Intelligent Automobiles

Surrounding all these promising advances, however, are very legitimate and important questions of privacy and security.

Our industry has every incentive to protect and maintain our customers' privacy because the next competitor is typically just a click away. While it is not that easy to click to another car, our companies have relationships they want to maintain across all product offerings. If a company loses a customer's trust as a result of one product, that customer is not likely to trust any other products offered by that company. One of the most critical components to protecting privacy and preserving customer trust is strong security.

ITI's member companies are at the forefront of providing security solutions for devices at the network edge, in the cloud, and everywhere in between. Security is not new for the technology sector; it has been in our blood for decades. With billions of additional devices coming online, ITI's companies are embedding security in IoT platforms at the outset of the manufacturing and design process for each new device that extends and expands the network. Security must be built into both hardware and software at the outset to ensure there are redundancies, to help prevent intrusions, and to create secure and trusted IoT systems that are more secure. Throughout the IoT, and particularly in the automotive space, technology companies are addressing security at the outset, an approach known as "security by design."

When designing for security, it is important to remember that advances in hardware technology allow for security to be physically built into a system. For example, semiconductor manufacturers can design chips with built-in safeguards. Encryption, for instance, can occur at the chip level. Manufacturers can also prevent chips from being rewritten by designing fuses into the chip. If a hacker attempts to access or rewrite the data, the fuse pops and prevents the data from being rewritten. Similarly, on the network side, vehicles communicating with the network will require a reliable level of service and connectivity, as well as high security to prevent unwanted intervention. New Internet protocol architectures are more adaptable and use advanced technologies to pervasively distribute security, treat individual users and devices with an appropriate level of performance and privacy based on their needs, and automate manual processes to improve scale and availability.

[13] *Id.* page 24.
[14] *Urban Mobility at a Tipping Point.*

Congress and the federal government have a critical role to play in fostering intelligent vehicle security. The tech sector has been partnered with the National Institute of Standards and Technology (NIST) for nearly three years as it developed what is commonly referred to as the NIST Framework for Improving Critical Infrastructure Cybersecurity (Framework).[15] The Framework stems from Executive Order 13636,[16] issued in February 2013, which called for the government to partner with owners and operators of critical infrastructure to improve cybersecurity through the development and implementation of risk-based standards. Development occurred through a process of coordination and collaboration led by NIST between the technology industry, others in private industry, and U.S. government partners. What resulted is a set of voluntary guidelines, best practices, and standards to help critical infrastructure, businesses, and other private and public actors to better manage cybersecurity risks. Taking a similar public-private partnership approach, NIST recently released a Draft Framework for Cyber-Physical Systems[17] (the "CPS Framework") that was developed in partnership with industry, academic, and government experts. For those like me, who do not regularly use the term "cyber-physical systems," it refers to networked objects, devices, and systems, or largely what we refer to as the Internet of Things. One of the key working groups in the cyber-physical systems project is focused on cybersecurity and privacy.

The Administration and NIST envisioned the Framework as applicable to helping organization across all critical infrastructure sectors, including the transportation sector, better secure their systems through risk management best practices and standards.[18] The CPS Framework is focused on identifying technical best practices and standards for building more secure cyber physical systems, including connected automobiles. Indeed, reviewing these and other major NIST projects - like those applying to workforce, privacy, authentication, vulnerability management, and risk management[19] – each contains elements that apply to different components of connected vehicle security. Most recently, NIST released a draft international cybersecurity standards strategy, which will soon be approved as official Administration policy that could easily embrace connected vehicles as IT Applications.[20]

---

[15] *See* NIST Framework for Improving Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/index.cfm

[16] *See* White House, Executive Order 13636, Improving Critical Infrastructure Cyber Security, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[17] *See* NIST CPS Draft Framework: http://www.cpspwg.org

[18] *See* White House, Presidential Policy Directive, Critical Infrastructure Security and Resilience, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[19] *See* NIST, Computer Security Division, Annual Report 2014, *rel.* August 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-176.pdf

[20] *Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objective for Cybersecurity*, NIST, http://www.nist.gov/itl/201508_cyber_standards_working_group_report.cfm See chart on Volume 2.

NIST also envisioned cross-agency coordination to ensure the NIST Framework fits the needs of each critical infrastructure sector, specifically stating "Sector-Specific Agencies…shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."[21]

At this point, you may be asking yourself why all this background is important. We believe it is pivotal for policymakers to continue to replicate this partnership approach in addressing IoT cybersecurity challenges. The NIST Framework provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all critical infrastructure sectors, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats. The cyber-physical systems framework will provide additional technical details for building secure products. On the flip side, viewing cybersecurity uniquely for each application, whether it be a home computer or an automobile, is inflexible and will leave industry less able to quickly and efficiently respond to new threats, potentially stifling innovation around security. As a first step to addressing cybersecurity, Congress, working with the respective agencies – NIST, Department of Homeland Security (DHS), and Department of Transportation (DoT) in particular for automotive safety – should evaluate the applicability of the NIST Framework to the automotive industry, possibly through a study led by an independent agency such as the Government Accountability Office (GAO) or the National Academy of Sciences (NAS). Then, if further action is necessary, legislation could be narrowly tailored to fill any gaps left by the Framework while still maintaining flexibility to address evolving threats and vulnerabilities.

Perhaps of more concern is the potentially counterproductive precedent of creating siloed approaches to cybersecurity across different IT applications, as part of the IoT and beyond. As more aspects of our daily lives increasingly become digitized, and more "things" are indeed connected to the internet in order to make our lives richer and more efficient, surely we don't need to reinvent the wheel when it comes to security, as each of these applications or use cases gains prominence. At different stages of the recent past, policymakers have considered whether new regulatory regimes were needed to better secure critical infrastructure, the electric grid, cloud computing, or health IT, and in each instance, after close examination, the benefits of approaches grounded in voluntary, consensus based international standards that can both promote innovation and preserve the promise of interoperability have carried the day. And NIST has consistently produced work bearing on all of these areas that we should leverage to benefit connected automobiles. The alternative – a world in which we endeavor to separately regulate each new IT application or IoT vertical – is unsustainable.

Another valuable role would be to ensure there is greater coordination and collaboration across information sharing and analysis centers (ISACs). The Automotive ISAC was formed about a year ago. Other industry ISACs have been in existence for longer periods of time – for

[21] EO 13636, Sec. 8(b).

instance the Information Technology ISAC (IT-ISAC) was formed in 2000 and was operational in 2001, and the Financial Services ISAC was launched in 1999 – and have developed best practices for effectively receiving and distilling threat information and working with the groups' members. The ISACS are invaluable to help address sector specific, and cross-sectoral threats and vulnerabilities. For example, the IT-ISAC helped monitor and collaborate with its members on large-scale threats such as Conficker and the DNS Cache Poisoning Vulnerability. The IT-ISAC provided a forum for members to engage in collaborative analysis on those significant issues, and to draft and share analytical alerts with remediation suggestions that were shared with members, partner ISACs and the public.

Congressional Support for Innovation

As promising and fast moving as innovations in intelligent transportation are, there are still many questions technology companies have that only Congress and the federal government can answer. Clarity and certainty around regulatory issues will enable greater investment and innovation by removing ambiguity about regulatory structures that may have been more applicable to "less-intelligent" vehicles of the past. Similarly, a forward-looking roadmap for intelligent vehicles and the IoT more generally, as well as policies that support that roadmap, will ensure continued U.S. leadership in this field. We urge policymakers to consider the following proposals:

Government coordination for emerging vehicular technology deployment – Conduct an independent government review and issue a public report, in consultation with the ICT sector, of existing federal automotive standards, regulations, and policies that present barriers to a competitive marketplace for safety and fuel efficiency technology breakthroughs, along with recommendations for removing or mitigating these barriers. Designate authority to specific federal agencies for IoT and intelligent transportation to prevent duplicative efforts across agencies. Conduct government engagement with international counterparts in the removal of regulatory barriers to safety and energy efficiency technology innovation.

Innovation and market development – Develop technology-neutral regulatory frameworks, when appropriate, to enable intelligent vehicle innovation. Using an industry-led approach, create voluntary global standards to accelerate adoption, drive competition, and enable cost-effective introduction of new technologies, while providing a clearer technology evolution path that stimulates investment.

Government planning and leadership – Create an advisory board with government and industry partners to produce a National IoT Strategy with ambitious timelines, and more tailored strategies for federal government adoption, smart city promotion, and promotion of next generation transportation. Intelligent vehicles and smart transportation should be viewed as a piece of this larger IoT strategy. Establish a new competitively selected National Network for Manufacturing Innovation (NNMI) hub dedicated to advanced ICT-enabled automotive and transportation technologies. Provide greater public availability of traffic information and open

transportation-related data to stimulate innovative new services and products for enhancing safety, fuel efficiency, and quality of life.

Conclusion

To realize the maximum potential of intelligent, connected, and autonomous vehicles, industry, Congress, the appropriate federal agencies, and policymakers around the globe must work collaboratively to create an environment that will allow for the full development of these technologies. There will be difficult issues to work through; the automotive sector is a historically regulated industry, whereas the tech sector has developed and thrived in large part because of flexibility to innovate and problem-solve without regulatory boundaries. But as all of the witnesses today testified, the potential for the "Internet of cars" is nearly limitless, and certainly was unimaginable just several decades ago. It will upend traditional business models, create new ones, and most importantly it is already providing safety and efficiency improvements to consumers which will only increase as these new technologies evolve and are ubiquitously adopted. On the business side, the tech sector is all-in to develop the technologies that will enable the intelligent, connected, and autonomous vehicles of the future; we stand ready to work with Congress and the appropriate federal agencies to ensure U.S. policies take us to that future.

Thank you again for the opportunity to testify, and I look forward to your questions.