

Division of Docket Management
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Deloitte Risk and Financial Advisoryⁱ comments in preparation of the Connected Cars -
Workshop, Project No. P175403

Dear Sir/Madam:

Deloitte Risk and Financial Advisory appreciates this opportunity to submit comments in preparation for the connected cars workshop to be held on June 28, 2017.

Cars today are programmed to transmit large volumes of data. A common example is vehicle speeds captured by navigational map applications (either on-board the vehicle or on mobile phones). Building upon this technology, insurance companies are encouraging their customers to install a device in the data port of their vehicles to gather statistics, such as average speeds, number of hard stops, and vehicle usage metrics to determine future insurance coverage and premiums. Another broad example of data collection (besides insurance company example above) is a map/navigational application that stores search and navigation history. Finally, as Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications mature, vehicles will share speed, heading, and other information directly with nearby vehicles and infrastructure (i.e., bridges or roads), which could result in a decreased number of accidents. The common theme in these examples is collection of more and more consumer data, much of which could be considered critical or confidential.

With the interoperability and interfacing of personal technology and increasingly sophisticated automotive technical capabilities, a massive amount of data is being created and collected; the connected automobile is no exception. In particular, due to the very personal nature of driving itself, a substantial amount of personally identifiable information (PII), such as driving habits and location information, is being created, processed, collected, and disposed by today's automobiles. This collected data allows for documentation of various personal habits, and needs to be protected while at rest, in transit, and when it is no longer needed (e.g., preferred driving routes). Manufacturers, consumers, and government agencies have a shared responsibility to ensure that true and sustainable privacy measures are designed into products and services as a core function. Security and privacy controls should complement, not impede the functionality of the service or product. Security and privacy should be incorporated early during product development and not be a bolt-on afterthought.

Deloitte Risk and Financial Advisory is the #1 risk and financial advisory practice in the world and provides a vast array of services to clients in many industries, including the Commercial and Industrial Products (C&IP) industry, of which Automotive is a sector. Within Automotive, we serve a well-rounded group of both US-based and global automotive Original Equipment Manufacturers

(OEMs), suppliers, and other mobility and technology-based organizations. In the cyber risk management space, we serve these clients by assisting them in solving very complex cybersecurity, privacy, and data protection and governance issues that sit at the intersection of technology, risk, and regulation.

As a result of our role serving the automotive industry and being a leader in cyber risk management, we have a distinct perspective the role that the Federal Trade Commission (FTC), the National Highway Traffic Safety Administration (NHTSA), and other government agencies could play with regard to privacy and security issues related to connected vehicles.

Deloitte Risk and Financial Advisory sees both the FTC and NHTSA as playing an active role with regard to life and safety issues that are at the heart of security and privacy in connected vehicles. For example, the FTC and NHTSA could recommend adoption of the National Institute of Standards and Technology (NIST) cybersecurity framework into a general automotive cybersecurity framework.

Such an automotive cybersecurity framework could provide interoperability among the industry stakeholders and government policy makers. The FTC and NHTSA can serve as important facilitators as industry, OEM, suppliers, government, and security experts jointly develop an industry-sponsored cybersecurity framework for the connected vehicle. In addition to this framework, an industry-government consortium could also serve as a research repository, providing enriched guidelines for data privacy, software and system security, and threat intelligence.

The combination of recommended adoption of an automotive cybersecurity framework and creation of an industry-government consortium is a layered approach to an interdependent set of issues. There could be multiple levels of governance that specify the interactions between OEMs, suppliers, state, local, and federal authorities. We applaud the FTC and NHTSA for their focus on collaboration between the public and private sectors.

A consortium approach could propose the overall cybersecurity framework for connected vehicles and could address specific needs such as vulnerability management, incident response, system security standards, data security standards, controls, and resiliency. For example, while connected vehicles may pass large volumes of data about vehicle performance and maintenance to the manufacturer, they could also be communicating roadway and safety information to local and state authorities. It is important that the public-level communications not disclose PII or other unnecessary information about the vehicle's occupants. Roadway data must be of the highest reliability and confidence, but also protect occupants' privacy. This confluence of needs introduces new disruptions in the transportation model that the FTC and NHTSA can be instrumental in addressing.

Deloitte Risk and Financial Advisory has demonstrated leadership in developing security guidance in public sectors including:

- Helped create the Federal Identity Credential and Access Management (FICAM) standards that implement Federal Information Security Management Act (FISMA).
- Sponsored and participated in voluntary policy models such as Food and Drug Administration's roundtables on secure medical devices that actively engaged industry and government.

- Helped develop the high-level guidance found in the NIST frameworks for security management, and understood the importance of keeping these standards as a “living approach” to adapt to the evolving ecosystem rather than to a static ruleset.

Deloitte Risk and Financial Advisory’s experience and interactions across the industry have identified the following focus areas as challenges to the connected vehicle ecosystem:

Life and Safety: In order to save lives, prevent injuries, and reduce the economic impact from vehicular incidents, many vehicle manufacturers are increasingly incorporating advanced driver assistance and safety components into vehicles. Because of the increasingly connected vehicle communication systems and their multiple attack surfaces, these advanced components are at increased risk of cyber-attack.

Data Privacy: The security of the vast amounts of sensitive data produced by the vehicle are another concern. The continuous desire to meet consumer demand and be first to market may prioritize rapid deployment and passenger safety over secure design. Anticipating that consumers will apply effective security controls by themselves is not an acceptable control; many consumers rarely change default device passwords or apply security patches. This makes security by design even more important.

Regulation: We understand that regulation does not always equate to security. Often, regulation becomes the minimum security standard, not the industry leading practice. The adoption of a common framework, such as the NIST cybersecurity framework, can align expectations and the ability to assess compliance with common industry standards.

We have provided a few examples of risks that we believe will resonate with your respective agencies, based on Deloitte Risk and Financial Advisory’s Cyber Risk experience with our “Secure.Vigilant.Resilient.TM” framework, targeting passenger safety and consumer data protection.

- **Secure** establishes risk-focused controls around their most sensitive assets, balancing the need to reduce risk, while also enabling productivity, business growth, and cost optimization objectives.
 - **Passenger Safety:** Concerns about tracking individual movements should be balanced against the need for vehicles to communicate traffic and roadway conditions that enhance safety for all drivers. Vehicles making autonomous decisions have to know that the data is accurate and authentic.
 - **Consumer Data:** Vehicle operations could require a substantial amount of PII including passenger data, destinations, entertainment preferences, and financial information, yet still necessitates appropriate protection.
- **Vigilant** services leverage deep experience with analytic and correlation technologies to help clients develop monitoring solutions focused on critical business processes. By integrating threat data, IT data, and business data, security teams are equipped with context-rich alerts to help prioritize incident handling and streamline incident investigation.
 - **Passenger Safety:** Security features must prevent unauthorized remote access to critical systems such as braking or steering. Vehicles making decisions based on traffic data have to be able to trust the data they receive to reduce traffic-related injuries and fatalities.

- **Consumer Data:** Consumers expect that the manufacturers are handling their data responsibly, preventing data loss via communications monitoring.
- **Resilient** services allow an organization's operations to rapidly adapt and respond to internal or external dynamic changes—opportunities, demands, disruptions, or threats—and continue operations with limited impact to the business.
 - **Passenger Safety:** Control systems must operate under reduced communications capacity or in an offline state to maintain vehicle control at all times. Rapid, consistent incident response requires the development of known incident response patterns for manufacturer and traffic monitoring systems and the links between them. War gaming and table top exercises conducted according to industry standards help mature new technologies for faster implementation.
 - **Consumer Data:** Data that is confidential must be available at all times and maintain its integrity and confidentiality across the entire data lifecycle.

Deloitte Risk and Financial Advisory appreciates the opportunity to provide these comments to the FTC and NHTSA, and we would welcome the opportunity to present our experience and point of view at the upcoming workshop. Should you have any questions regarding our comments, please contact us.

Respectfully submitted,

Joseph Kwederis
Principal | Deloitte Risk and Financial Advisory
Automotive Leader, Cyber Risk Services
Deloitte & Touche LLP
jkwederis@deloitte.com

Sean Peasley
Partner | Deloitte Risk and Financial Advisory
Consumer & Industrial Products Leader, Cyber Risk Services
Deloitte & Touche LLP
speasley@deloitte.com

¹As used in this document, "Deloitte Risk and Financial Advisory" means Deloitte & Touche LLP, which provides audit and risk advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Disclaimer: This document contains general information only and Deloitte Risk and Financial Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Risk and Financial Advisory shall not be responsible for any loss sustained by any person who relies on this document.