Connected Cars Workshop

STAFF PERSPECTIVE | JANUARY 2018

Introduction

Modern motor vehicles increasingly are equipped with technologies that enable them to access information via the Internet and gather, store, and transmit data for entertainment, performance, and safety purposes. Automated vehicles, those with vehicle-to-vehicle (V2V) communications technology, and other forms of wireless connectivity can provide important benefits to consumers and have the potential to revolutionize motor vehicle safety. At the same time, these technologies raise privacy and security concerns.

On June 28, 2017, the FTC and the National Highway Traffic Safety Administration (NHTSA) hosted a workshop in Washington, DC to discuss these issues. The day-long event featured representatives from consumer groups, industry, government, and academia, and explored the benefits and challenges of this growing market and its effect on consumer privacy and cybersecurity.

Key Takeaways

Several important points emerged from the workshop. First, many companies throughout the connected car ecosystem will collect data from vehicles, much of which will be used to provide important benefits to consumers. The car manufacturers themselves will collect data for a variety of purposes, such as to provide services for vehicle owners. For example, they may collect precise geolocation data to direct emergency personnel to the scene of a crash. To ensure safe operation and to prevent crashes, they may also broadcast location information to each other in real time. In addition, manufacturers of infotainment systems on vehicles will use data to enable consumers to use apps such as navigation or music apps, access their contacts, or connect to the Internet. Finally, some third parties provide "dongles" that connect to a port in cars, which collect and transmit consumer data. Such data may include information about consumer driving habits, such as if a driver regularly speeds or slams on the brakes. As one workshop participant noted, some of this information can be used for diagnostic purposes, to indicate a vehicle's state of health and determine whether certain subsystems are behaving properly. Other participants noted that auto insurance companies can use this information to determine rates for consumers: consumers who demonstrate good driving habits can qualify for insurance discounts. Some participants viewed this use as a benefit rewarding safer driving; others were concerned about the potential for insurance companies to use this information, without consumers' knowledge, to raise rates, or to penalize safe drivers who choose not to authorize the collection of information.

Second, the types of data collected through connected cars will range from aggregate data, to non-sensitive data about a particular vehicle or individual, to sensitive personal data. For example, aggregate information can be used for traffic management to reduce congestion. Non-sensitive personal data can be used to measure a particular car's gas mileage or how it performs in different driving conditions such as rain and snow. Vehicles might also collect sensitive data about the occupants of the vehicle themselves, such as a fingerprint or iris pattern for authentication purposes, or information about the vehicle's – and the occupants' – real-time location.

Third, given all of this data collection, consumers may be concerned about secondary, unexpected uses of such data. For example, personal information about vehicle occupants using the vehicle's infotainment system, such as information about their browsing habits or app usage, could be sold to third parties, who may use the information to target products to consumers. While some consumers may welcome product recommendations based on their interests, others may have concerns about recommendations based on, for example, tracking of their usage of apps.

The participants noted that addressing consumer privacy concerns is critical to consumer acceptance and adoption of the emerging technologies behind connected cars. Industry

initiatives, such as the Consumer Privacy Principles jointly introduced by the Alliance of Automobile Manufacturers and Global Automakers in 2014, are an important step in this process. Similarly, the National Automobile Dealers Association has partnered with the Future of Privacy Forum to produce consumer education that explains the kinds of information that may be collected by consumers' cars, the guidelines that govern how it is collected and used, and the options consumers may have. Some consumer advocates expressed concern, however, that it is not easy for consumers to figure out what kind of information their cars may be collecting or sharing and suggested the development of a central portal where consumers could compare automakers' different privacy policies.

Participants suggested that different approaches may be needed depending upon whether the data in question is safety-critical or not. For example, V2V and automated safety technologies will require vehicles to regularly transmit "Basic Safety Messages" about their speed, direction, brake status, and other vehicle information to surrounding vehicles, and receive the same information from them. That information is necessary for the safe operation of all vehicles on the road. In such cases, consumers' ability to opt out of such information sharing may not be appropriate. Other data, such as the data generated when a consumer syncs her smart phone to the car's infotainment system to access her phone book, are not safety-critical. In those instances, participants agreed that consumers should be provided with clear, easily understandable information about if and how their information is being collected, stored, or transmitted and how they can access or delete that information.

Fourth, connected and autonomous vehicles will have cybersecurity risks that can potentially be exploited. Before cars' computer systems were connected to the internet, a hacker needed physical access to a vehicle's computer network to extract information from it or control vehicle functions; with connectivity, a hacker could potentially access one or more vehicles remotely. Moreover, attackers have become more sophisticated. After a group of attackers has done the work to identify an attack vector, they may share that attack publically, simplifying follow-up attacks. Several workshop panelists raised the possibility of remote attacks that could involve large numbers of connected vehicles.

Panelists proposed a variety of possible motivations for attacks on connected networks in vehicles, ranging from everyday hackers seeking thrills, notoriety, or monetary gain to nation-states seeking to create chaos by taking vehicle control away from drivers, possibly leading to physical harm to vehicles and their occupants. Panelists identified some best practices for addressing these risks:

- *Information sharing*: Panelists agreed that information sharing through groups such as the Auto-ISAC, the International Organization for Standardization, and the Society of Automotive Engineers may limit the

extent to which vulnerabilities can be exploited. The FTC has encouraged such information sharing.

- *Network design*: Panelists discussed connected car network design solutions, such as segregating safety-critical functions from other functions controlled through the networks.
- *Risk assessment and mitigation*: Panelists discussed risk assessment and mitigation practices during vehicle development and after sale, and explored solutions for addressing newly discovered vulnerabilities, including over-the-air updates to connected networks.
- *Standard setting*: Panelists discussed the importance of industry self-regulation, including efforts to create security best practices, and government standards and guidance, such as the NIST framework, in helping to set baseline security for connected cars.

Developments Since the Workshop

FTC staff notes that there have been some important developments since the workshop. On September 6, 2017, the U.S. House of Representatives unanimously passed H.B. 3388, the Safely Ensuring Lives Future Development and Research in Vehicle Development (SELF DRIVE) Act to encourage the testing, development and deployment of highly automated vehicles ("HAVs") in the United States. Among other things, the bill requires the manufacturers of HAVs to develop a written cybersecurity plan that includes vulnerability detection and response practices and a process for controlling access to automated driving systems. The bill also requires NHTSA to develop a rulemaking plan for HAV safety standards and directs the FTC to conduct a study and submit a report regarding the HAV marketplace.

And on September 12, 2017, the U.S. Department of Transportation and the NHTSA released new federal guidance for automated vehicles, *Automated Driving Systems 2.0: A Vision for Safety*, which provides voluntary guidance that encourages best practices and prioritizes safety. The document also provides technical assistance to states and best practices for policymakers. Although the document does not directly address privacy, the accompanying Q&A notes the important role of the FTC in protecting consumer privacy in the connected car space.

Conclusion

The FTC staff is grateful to the workshop participants for sharing their views. We will continue to monitor the connected car marketplace, using our civil authority to protect consumers from unfair or deceptive practices, looking for opportunities to educate consumers and businesses, and working with stakeholders to foster innovation while protecting the privacy and security of consumer information.

Video of the workshop in its entirety can be found on our website at https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.