FTC and NHTSA Seek Input on Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles

Agencies to Conduct Workshop on June 28, 2017

Modern motor vehicles increasingly are being equipped with technologies that enable them to access information via the Internet and gather, store and transmit data to provide entertainment, improve performance and promote safety. These vehicle systems will only become more complex in the future, with increased functionality. In the near future, the National Highway Traffic Safety Administration (NHTSA) may mandate vehicle communication systems that wirelessly exchange safety data with nearby vehicles to warn drivers of collision risks (vehicle-to-vehicle or V2V systems). These systems also may enable vehicles to communicate with roadway infrastructure (vehicle-to-infrastructure or V2I systems) to enhance safety, mobility and the environment. In addition, increasingly automated vehicles (in which at least some safety-critical control or function happens without the intervention of a human driver) are expected to become more prevalent in the marketplace.

Automated, V2V- and V2I-enabled, and other connected vehicles (i.e. with some form of wireless connectivity) can provide important benefits to consumers and have the potential to revolutionize motor vehicle safety. At the same time, these vehicles are expected to generate an enormous amount of data, some of which will be highly personal and sensitive, such as geolocation data and contents of communications that result from drivers connecting their phones to their vehicle' "head units." For example, according to Fortune magazine, by 2020, autonomous vehicles will generate about 4,000 gigabytes of data a day – the data equivalent of almost 3,000 people through use of their PCs, mobile phones and wearables, according to Intel (by comparison, the average person today generates about 650 MB of data a day).[1] These Internet-connected vehicles face many of the same security vulnerabilities as other connected computing platforms. Protecting the security of these vehicle technologies is crucial to maintaining adequate privacy and safety protections.

The Federal Trade Commission and NHTSA are exploring the consumer privacy and security issues posed by "connected vehicles," including vehicles currently on the road, V2V- and V2I-equipped vehicles, and automated vehicles. The FTC invites comments on these issues in advance of a public workshop to be held at the FTC's Constitution Center Building, 400 7th Street, SW, Washington, DC on June 28, 2017 in Washington, D.C. An agenda for the workshop will be made available later on the FTC's website.

To aid our analysis of these issues and various proposals intended to address them, FTC and NHTSA staff seek input on the privacy and security issues associated with these connected vehicles. Topics of interest to the FTC include, for example:

- What data do vehicles with wireless interfaces collect/store/transmit, and how is the data used and shared?

[1] http://fortune.com/2016/11/15/intel-is-making-a-major-investment-in-autonomous-vehicles/

- How do these vehicles integrate data into their functionality? How do consumers benefit from the collection and use of their information?
- What are the current roles of vehicle manufacturers, parts suppliers, technology companies, and other stakeholders in collecting data and ensuring security? How are these roles expected to evolve?
- What are the vehicle manufacturers' privacy and security policies and practices? How are those policies and practices communicated to consumers? What choices are consumers given about how their data is collected, stored, and used? Who owns the data?
- What, if any, privacy and security harms can arise from connected vehicle manufacturers and their service providers' collection and use of data? What is the likelihood of such harms?
- What privacy and security issues might arise from consumer operation of connected vehicles, including use of third-party aftermarket products that can plug into vehicle diagnostic systems, geolocation systems, or other data-generating aspects of connected vehicles?
- What evidence exists regarding consumer perceptions of connected vehicles and their data collection and use practices?
- What are the roles of the FTC, NHTSA, and other federal government agencies with regard to the privacy and security issues concerning connected vehicles?
- What self-regulatory standards apply to privacy and security issues relating to connected vehicles?

FTC and NHTSA staff welcomes comment on these and related questions and issues. The FTC will accept submissions through April 20, 2017. Interested parties may file a comment online or on paper. Write "Connected Cars Workshop and P175403" on your comment and file your comment online at https://ftcpublic.commentworks.com/ftc/connectedcarsworkshop by following the instructions on the web-based form. If you prefer to file your comment on paper, write "Connected Cars Workshop and P175403" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex A), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex A), Washington, DC 20024. The FTC requests that any paper submissions be sent by courier or overnight service, if possible, because postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions.

Your comment - including your name and your state - will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Website, at https://www.ftc.gov/policy/public-comments. As a matter of discretion, the Commission tries to

remove individuals' home contact information from comments before placing them on the Commission Website. Because your comment will be made public, you are solely responsible for making sure that your comment does not include any sensitive personal information, like anyone's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, like medical records or other individually identifiable health information. In addition, do not include any "[t]rade secret or any commercial or financial information which . . . is privileged or confidential," as discussed in Section 6(f) of the FTC Act, 15 U.S.C. § 46(f), and FTC Rule 4.10(a)(2), 16 CFR § 4.10(a)(2). In particular, do not include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names. If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you have to follow the procedure explained in FTC Rule 4.9(c), 16 CFR § 4.9(c). Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest.

The Federal Trade Commission develops policy initiatives on issues that affect competition, consumers, and the U.S. economy. Like the FTC on Facebook, follow us on Twitter, and subscribe to press releases for the latest FTC news and resources.