WILMERHALE

FTC Staff Releases Paper Highlighting Key Privacy and Security Issues for Autonomous and Connected Vehicles

JANUARY 17, 2018

The Federal Trade Commission Staff (FTC) released a new "Staff Perspective" on January 9, 2018, that highlights key privacy and data security issues related to autonomous and connected vehicles. The Staff Perspective outlines four key takeaways from a workshop hosted by the FTC and the National Highway Traffic Safety Administration (NHTSA) on June 28, 2017. It also summarizes recent legislative and regulatory developments and indicates that the FTC will continue to monitor the connected car marketplace. Companies that manufacture or integrate with connected car technology should keep a close eye on future FTC actions in this marketplace, and they should understand that the FTC expects businesses to protect the privacy and security of information relating to consumers when collecting, using, or sharing data through connected cars.

We summarize below the FTC's key takeaways from the workshop.

1. Many companies throughout the connected car ecosystem will collect data from vehicles, much of which will be used to provide important benefits to consumers

First, the Staff Perspective notes that many different entities will collect data from connected vehicles, including car manufacturers, manufacturers of "infotainment" systems, third parties that provide peripherals that plug into ports on cars, and auto insurance companies. This observation should not be surprising given the proliferation of Internet-connected devices and the increasing use of advanced navigation, safety, and entertainment technologies in modern vehicles.

The Staff Perspective also notes that much of the data will be used to provide important benefits to consumers. This suggests that FTC Staff will balance the potential benefits of connected car technologies against the privacy and data security concerns that arise from the increased collection, use, and sharing of data. However, the Staff Perspective also cautions that workshop participants disagreed on whether certain uses—such as providing "good driver" discounts to consumers who demonstrate good driving habits—would ultimately benefit or harm consumers. The Staff Perspective does not weigh in on the lawfulness of specific practices, but we expect that the FTC Staff will keep a close eye on any new uses of data in the connected car ecosystem and will scrutinize any practices that it views as potentially unfair or deceptive, in violation of Section 5 of the FTC Act.

2. 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

Second, the Staff Perspective emphasizes that companies will collect various types of data through connected cars, including aggregate data, non-sensitive data about a particular vehicle or individual, and sensitive personal data. The Staff Perspective notes, for example, that entities may collect and use aggregate data for traffic management to reduce congestion or may collect and use non-sensitive personal data to measure a particular car's gas mileage. Sensitive data would include information "such as a fingerprint or iris pattern for authentication purposes, or information about the vehicle's – and the occupants' – real-time location."

These distinctions regarding the types of data collected are important. For example, in prior guidance, the FTC has cautioned that companies must obtain *affirmative express (e.g., opt-in) consent* from consumers before collecting, using, or sharing *sensitive* information (such as precise location data, health data, financial data, data regarding children, and data regarding consumers' television viewing habits). Further, if non-sensitive data can be reasonably linked to a specific consumer, computer, or other device (such as a vehicle or its computer systems), the FTC has indicated in prior guidance that companies should follow the privacy framework outlined in its 2012 report titled Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers ("2012 Privacy Report"). The FTC's privacy framework contains detailed principles that call for privacy-by-design, increased transparency, and simplified consumer choice.

3. Consumers may be concerned about secondary, unexpected uses of data

Third, the Staff Perspective cautions that consumers may be concerned about secondary, unexpected uses of data. For example, the Staff Perspective notes that some consumers may have concerns if personal information collected through a vehicle's infotainment system—such as information regarding the occupants' browsing habits or app usage—were sold to third parties for targeted advertising purposes. The Staff Perspective notes that workshop participants agreed that it is critical to address such consumer privacy concerns in a manner that encourages acceptance and adoption of the emerging technologies behind connected cars.

To address such privacy concerns, the Staff Perspective appears to support self-regulation in the connected car industry (at least for the moment), which is consistent with the regulatory approach that the FTC Staff has taken in other industries, such as the online behavioral advertising industry. For example, the Staff Perspective notes that the Consumer Privacy Protection Principles for Vehicle Technologies and Services were jointly introduced by the Alliance of Automobile Manufacturers and Global Automakers in 2014 and that such industry initiatives are "an important step" in addressing privacy concerns in the connected car ecosystem. Those self-regulatory guidelines—which apply to participating automakers but do not apply directly to third-party service providers, app providers, or independent dealerships—are based on the following broad principles:

- **Transparency**: Participating members commit to providing owners and registered users with ready access to clear, meaningful notices about the participating member's collection,

use, and sharing of covered information;

- **Choice**: Participating members commit to offering owners and registered users with certain choices regarding the collection, use, and sharing of covered information;
- **Respect for Context**: Participating members commit to using and sharing covered information in ways that are consistent with the context in which the covered information was collected, taking account of the likely impact on owners and registered users;
- **Data Minimization, De-Identification & Retention**: Participating members commit to collecting covered information only as needed for legitimate business purposes. participating members commit to retaining covered information no longer than they determine necessary for legitimate business purposes;
- **Data Security**: Participating members commit to implementing reasonable measures to protect covered information against loss and unauthorized access or use;
- **Integrity & Access**: Participating members commit to implementing reasonable measures to maintain the accuracy of covered information and commit to giving owners and registered users reasonable means to review and correct personal subscription information; and
- **Accountability**: Participating members commit to taking reasonable steps to ensure that they and other entities that receive covered information adhere to the Principles.

The Staff Perspective also notes, however, that some consumer advocates at the workshop expressed concern that it is not easy for consumers to understand companies' information practices and that it would be helpful to develop a central portal where consumers could compare automakers' different privacy policies. These concerns suggest that, in the future, the FTC Staff and consumer privacy advocates may scrutinize whether privacy notices and choices offered to consumers are sufficiently clear and prominent and are provided at a time and in a context in which the consumer is making a decision about his or her data (*e.g.*, "just-in-time" notices that appear outside of the privacy policy).

For example, in the context of online behavioral advertising, where information about a user's web browsing and mobile app usage history across unaffiliated websites and mobile apps is used to deliver targeted advertising to the user, the FTC and self-regulatory organizations have encouraged companies to design innovative ways, outside of the privacy policy, to provide disclosures and choices to consumers. (*See, e.g.*, the FTC Staff's 2009 Report on Self-Regulatory Principles for Online Behavioral Advertising ("OBA") and the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising). The online advertising industry has implemented such guidance by adopting an easily-recognizable "AdChoices" icon that participating companies may display in or around advertisements that are delivered using OBA data, and which links to the company's privacy policy notice and an opt-out mechanism. This allows consumers to easily learn more and make choices about potentially unexpected uses of their web data for targeted advertising purposes.

The Staff Perspective also notes that, in the connected car ecosystem, different approaches may be necessary depending on whether data is safety-critical or not. For example, the Staff Perspective indicates that it may not be appropriate to provide consumers with the ability to opt out of sharing

safety-critical data with surrounding vehicles, such as vehicle-to-vehicle communications that regularly transmit "Basic Safety Messages" about speed, direction, brake status, and other vehicle information. However, the Staff Perspective notes that data generated from a consumer's interactions with infotainment systems are not safety-critical. In such cases, the Staff Perspective notes that participants in the workshop 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."

4. Connected and autonomous vehicles will have cybersecurity risks that can potentially be exploited

Fourth, the Staff Perspective emphasizes that connected and autonomous vehicles will have cybersecurity risks that can potentially be exploited. The FTC Staff's data security concerns focus on hackers' ability to access vehicles remotely, to share attack vectors in a manner that would simplify follow-up attacks, and to launch attacks that affect a large number of connected vehicles. To address such risks, the Staff Perspective notes that workshop panelists recommended increasing information sharing, improving network design, conducting risk assessment and mitigation, and setting standards for baseline security in connected cars.

5. Developments since the workshop

Finally, the Staff Perspective notes that there have been other important developments since the FTC and NHTSA held the workshop last year. For example, the Staff Perspective notes that the U.S. House of Representatives unanimously passed H.B. 3388, the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution (SELF DRIVE) Act, and that the U.S. Department of Transportation and the NHTSA released new guidance for automated vehicles, titled *Automated Driving Systems 2.0: A Vision for Safety*.

The Staff Perspective notes that the SELF DRIVE Act would require manufacturers of "highly automated vehicles" to develop a written cybersecurity plan that includes, among other things, vulnerability detection and response practices and a process for controlling access to automated driving systems. The Staff Perspective also notes that while the NHTSA's new guidance does not directly address privacy, the NHTSA's Q&A document accompanying the new guidance highlights the important role of the FTC in protecting consumer privacy in the connected car industry.

Looking forward

The FTC's Staff Perspective indicates that FTC Staff will continue to monitor the connected car marketplace. At least for the moment, FTC Staff appears willing to allow individual companies and self-regulatory programs to continue developing privacy and security principles and best practices for connected car technologies. In the meantime, however, the Staff Perspective also notes that the FTC Staff will use its civil authority under Section 5 of the FTC Act to bring enforcement actions against companies that engage in unfair or deceptive practices, such as if a company makes materially false or misleading statements to consumers regarding its privacy or data security practices or fails to have "adequate security protections," as described in the FTC's Start with

Security guidance document and its Stick with Security Blog series.

Given the abundance of data collection, the concerns about secondary uses of data that may be unexpected by reasonable consumers under the circumstances, and the potential for significant cybersecurity risks, the Staff Perspective highlights the need for companies in the connected car ecosystem to be proactive and to build privacy and security into their products at every stage of development. In this regard, companies should review the FTC's 2012 Privacy Report and subsequent reports that address privacy and security issues in more traditional contexts, and they should think strategically about additional steps they can take to address privacy issues that are unique to connected car technologies.