Published on *The National Law Review* https://natlawreview.com

Parties Discuss Privacy Issues in Advance of FTC, NHTSA Workshop on Connected Cars

Article By:

Hannah Lepow

Automated vehicle technology is accelerating, and regulators are racing to keep up. On June 28, 2017, the Federal Trade Commission and the National Highway Traffic Safety Administration ("NHTSA") will hold a workshop to examine the consumer privacy and security issues posed by automated and connected vehicles. The workshop comes several months after the Department of Transportation and NHTSA promulgated a Notice of Proposed Rulemaking ("NPRM") that would require all new passenger vehicles to be capable of vehicle-to-vehicle ("V2V") communications by the early 2020s.

The FTC and NHTSA have raised several questions to be addressed at the workshop, including:

- What data do vehicles with wireless interfaces collect, store, and transmit, and how is that data used and shared?
- What are vehicle manufacturers' privacy and security policies and how are those policies communicated to consumers?
- What choices are consumers given about how their data is collected, stored, and used?
- What are the roles of the FTC, NHTSA, and other federal agencies with regard to the privacy and security issues raised by connected vehicles?
- What self-regulatory standards apply to privacy and security issues relating to connected vehicles?

Car manufacturers, tech organizations, privacy organizations, and other parties filed comments in advance of the workshop, responding to these questions and more:

- The Association of Global Automakers, a group that includes Aston Martin, Ferrari, Honda, Toyota, and others, said that V2V and vehicle-to-infrastructure ("V2I") communications do not present a significant privacy risk to individuals because they do not collect or store PII or

information that can be linked to a particular vehicle. The organization stated that the method of communicating between cars—dedicated short range communications ("DSRC")—"already has layers of security established into its design." The group did acknowledge that privacy and security issues "may be exacerbated" by wireless-enabled aftermarket products connected to on-board diagnostics ports, and said that developers and third parties should therefore take appropriate steps to design and manufacture secure products.

- CTIA praised the safety benefits that connected vehicle technologies could provide, highlighting how 5G network speed, capacity, and location can improve autonomous vehicle safety and efficiency. The wireless group spoke to both its sector's experience in addressing data privacy and security across the Internet of Things, and urged the agencies to refrain from imposing vehicle-specific privacy or security regulations which "could be redundant to or conflict with existing privacy and data security protections enforced by the FTC and the Department of Homeland Security." CTIA instead said the agencies should promote and expand industry-led initiatives like the NIST Cybersecurity Framework and self-regulatory principles like the auto industry privacy principles.

- In contrast, EPIC said that "meaningful oversight and enforcement mechanisms" would be necessary to protect consumer privacy. In its discussion of federal policies, the organization stated that enforcement would "require[] a private right of action against companies who misuse and fail to secure personal information." The organization also opposed the NPRM's proposal to create a new Federal Motor Vehicle Safety Standard ("FMVSS") which would preempt state regulations, arguing that historically, while the federal government has enacted privacy laws, more robust privacy legislation has been implemented at the state level.

- The Future of Privacy Forum, which runs a Connected Cars Working Group whose members include Fiat Chrysler, Ford, General Motors, Hyundai, Lyft, Toyota, and Uber, urged the agencies to focus on transparency around consumer data use, including the provision of resources that are publicly available, accessible before purchase, and reviewable throughout the life of a vehicle as well as the incorporation of consumer privacy controls when appropriate. The group urged the agencies to encourage industry self-regulatory efforts, saying that they can be enforceable when companies publicly commit.

National Law Review, Volume VII, Number 131