Summer Road Trippin': The FTC and NHTSA Workshop on Connected Cars

Kristi L. Wolff

July 5, 2017

On June 28, the FTC and National Highway Traffic Safety Administration (NHTSA) brought together a variety of stakeholders including regulators, automakers, software companies, and consumer groups to discuss connected cars, including current innovations and challenges in the field of data privacy. Acting FTC Chairwoman Maureen Ohlhausen opened the day by asserting that regulators will need to show "humility" in trying to understand the risks associated with connected cars. However, she emphasized that the FTC will still use their enforcement authority against those who misuse consumer data, while taking care not to conflict with NHTSA's oversight efforts. Terry Shelton, acting executive director of NHTSA, agreed with these goals. The day's panels focused on three main themes:

Safety – Fewer Accidents, Better Recall Compliance, and Privacy

Connected cars are expected to be able to decrease accidents and traffic fatalities. According to Terry Shelton, Acting Executive Director of NHTSA, 94% of fatal car accidents are due to human error. Additionally, both Shelton and Acting FTC Chairwoman Ohlhausen emphasized that the number of automobile-related fatalities has risen considerably in recent years.

It is less clear what happens when the artificial intelligence (AI) systems responsible break down. As cars become better able to make decisions on their own, the question of liability when a mistake occurs will be brought to the forefront. However, connected cars may increase compliance with safety recalls as self-driving cars may bring themselves into the shop for repair, and manufacturers will more easily be able to trace automated cars that have not been updated. The panel also discussed whether consumers should be allowed to opt out of sharing safety data and whether safety concerns may be used as excuses to collect information for commercial use.

Data – Notice and Consent, Types and Use of Data

As is the case with all connected devices, data collection and use presents many questions. Current technology allows devices to use driving patterns to detect drowsy driving, but newer devices will use biometric data for this purpose. Depending on how the data is gathered, mechanisms for consumer notice and consent remain a challenge.

Stephen Pattison of ARM offered three important categories of data that may be taken from connected vehicles. The first is information linking the user to the vehicle. He asserted that this is the most sensitive information, and should be controlled by the consumer. The second is information that is brand sensitive, and may be of interest to competitors. This also includes information about individual components of the car. It will be up to the manufacturer how and when this information is

shared. The third category is non-identifying information such as road conditions. This information is useful for other companies and law enforcement to use under some agreement that outlines the terms of use.

Panelists noted that the information produced by these vehicles is not encrypted or anonymized, as doing so would destroy the value of the data. It is important for the car or car system to be able to understand why a mistake occurred, or be able to make choices using very granular data, and share that data either with itself or in vehicle to vehicle communications to make other cars smarter and more able to make those decisions as well.

After-market products that are purchased by consumers and voluntarily placed into their cars are also collecting data. These include devices such as remote start, backup cameras, or an insurance dongle. While there is more consumer acknowledgement that these devices will be tracking personal information, the panelists at the workshop were in general agreement that more information should be given to consumers in clear and concise ways to enable them to make informed choices.

Security and Privacy – It's Not If, But *When* A Breach Will Happen

One phrase that was repeated during the conference was: it is not a question of if, but *when* a breach will happen. Carrie Morton of the University of Michigan's Mcity automated-vehicle research center explained that consumers are often "okay with the tradeoff" of exposing their personal driving information if they see a benefit. However, there is some information that even the most connected of drivers do not want exposed. While it may be true that consumers care less about who has their data is than what is being done with it, this cannot be mistaken for a lack of care concerning data privacy in general.

Earlier this year, NHTSA released a set of best practices to protect connected cars against cyberattacks and data breaches. These included a push for earlier integration of breach detection, a feature which Jeff Massimilla of GM said they are building into their cars from the beginning. NHTSA will look to the FTC for support in enforcing these regulations. There was also support from some panelists for harsher FTC sanctions for those that unlawfully access or re-identify anonymized data, as the data will likely be easy to de-anonymize.

* * *

We'll continue to follow these issues and related connected product developments here at Ad Law Access.