WILMERHALE

FTC and NHTSA Navigate Privacy and Security Issues at "Connected Cars" Workshop

JULY 5, 2017

The majority of new cars today come with a variety of so-called "connected" features, such as the ability to communicate with one another, Internet-connected features and video content, and even the ability to drive themselves. These "smart" cars collect, use, and share vast amounts of data and, as a result, prompt a host of privacy and data security issues. On June 28, 2017, the Federal Trade Commission (FTC) and National Highway Traffic Safety Administration (NHTSA) held a workshop to examine such issues and to discuss the benefits, risks, and roles of various stakeholders as connected car technologies continue to evolve. The FTC Staff, alone or in combination with NHTSA Staff, may (as they often do following workshops on new technologies or new uses of existing technologies) issue a report or other business guidance over the next several months, and we anticipate that NHTSA will incorporate ideas expressed at the workshop into its own rules and guidance going forward, such as in its Notice of Proposed Rulemaking on vehicle-to-vehicle ("V2V") communications. In the meantime, companies can look to existing FTC guidance and self-regulatory principles and best practices, including the Consumer Privacy Protection Principles for Vehicle Technologies and Services and the Automotive Cybersecurity Best Practices.

The FTC/NHTSA workshop included opening remarks from federal regulators and a series of panel discussions that brought together agency staff, industry representatives, privacy advocates, and academics. The workshop revealed how deeply stakeholders in the automotive space are thinking about privacy and data security issues and the regulatory challenges associated with connected and autonomous vehicles.

Regulatory Approaches

To begin the workshop, regulators at the FTC and NHTSA described their approaches to addressing privacy and security issues raised by connected cars. In her opening remarks, Acting FTC Chairman Maureen Ohlhausen highlighted the potential benefits of connected cars and emphasized that the FTC's approach is one of "regulatory humility." Predicting the future is difficult, she said, and understanding the benefits and risks is critical in any decision to enforce privacy and security standards in the industry. She noted that in 2016, for instance, the National Safety Council estimated that roughly 40,000 deaths occurred due to car accidents, a figure that could be significantly reduced

by V2V communications technology. Chairman Ohlhausen stressed that regulators must be careful not to hinder such positive developments with unnecessary or duplicative regulations. To be certain, however, she also warned that the FTC will use its enforcement authority under Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, in appropriate circumstances. She highlighted the FTC's prior privacy and data security enforcement actions involving Internet-connected routers, cameras, and TVs, and she noted that the FTC could take action against manufacturers *and* service providers that collect, use, or share data through connected cars. In addition, she repeated the FTC's longstanding calls for Congress to pass data security and data breach notification legislation (which potentially could include FTC rulemaking authority and, thus, the ability to seek and enforce civil penalties) and to strengthen the FTC's existing enforcement tools.

Terry Shelton, Acting Director of NHTSA, emphasized the role of government in encouraging private-sector partners to independently develop appropriate safety features and standards. She further called for the FTC and Department of Transportation (DoT) to enforce consumer protection standards and work with stakeholders to ensure that innovation does not ultimately intrude upon consumer privacy. Similarly, Thomas Buhl, Acting Director of the FTC's Bureau of Consumer Protection, alluded in brief closing remarks to the need for constant communication between government agencies, cybersecurity experts, trade associations, and other stakeholders in crafting thoughtful guidance and self-imposed industry standards.

Indeed, several participants acknowledged that many important changes have been led by industry rather than imposed by agencies. Nat Beuse, Associate Administrator of Vehicle Safety Research at NHTSA, pointed out that automatic braking will become standard as soon as 2022—an industry move rather than a regulatory requirement—and that regulators should not be in the business of picking technological winners and losers. Jeff Massimilla, Chief Product Cybersecurity Officer for General Motors, also pointed out that the Automotive Information Sharing and Analysis Center (commonly known as the "Auto ISAC," an industry consortium comprised of manufacturers, suppliers, and fleet/carrier companies dedicated to enhancing collaboration and awareness of automotive cybersecurity issues) has produced Automotive Cybersecurity Best Practices and routinely shares data on cybersecurity threats among its members.

What Are Connected Cars, and What Data Do They Collect, Use, and Share?

The workshop's detailed public notice described connected cars as vehicles "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." The workshop's first panel discussion explored how such connected cars collect, use, and share data.

Cars, like many consumer devices today, are increasingly reliant on the Internet and other communications technologies to maximize their usefulness. For example, modern cars already contain several desktops' worth of computing power. These computerized functions include everything from measuring speed, checking tire pressure, optimizing fuel economy, and maintaining engine temperature. Newer models come with Internet-connected dashboards and TVs, phones that connect to emergency services in case of an accident, ignitions or doors that are activated

through a smart watch, sensors that look for nearby cars, and cameras that help park or navigate the vehicle. These features transmit data and, according to some estimates, by 2020 a single car will produce 30 terabytes of information daily.

Industry representatives at the workshop further explained that data is transmitted to a variety of entities and in a variety of ways. For example, V2V and vehicle-to-infrastructure ("V2I") technologies collect and package safety-related data, such as speed, direction, and location, through radar, cameras, and other sensors. Vehicles then transmit this data to all compatible V2V or V2I devices nearby. The intended recipient may be a nearby driver, who would know if another car has suddenly braked, or a nearby traffic light. Other information, such as authentication data used for unlocking doors or logging into Facebook, may be shared with manufacturers, service providers, or the car itself through infrared and satellite signals.

Researchers and experts noted that the types of information collected differ in fundamental ways and may raise unique privacy and security risks. For example, precise location data, which the FTC has traditionally viewed as sensitive data that requires users' affirmative express consent to collect, may be generated through V2V signals or through normal satellite channels, much like GPS tracking on smartphones. However, these data differ in meaningful ways from other data that may be collected through connected cars, including biometric data (such as voice or fingerprint recognition), behavioral data (such as driving patterns, speed, acceleration, or vehicle stability), or personally identifiable information (such as a name, phone number, or username and password).

Panelists generally agreed that the potential uses of data in connected cars promise many benefits, including reduced road congestion, pollution, and fatalities, as well as more time for productivity or leisure. Geolocation data, for instance, is already used by companies like Google Maps and Waze to provide real-time information regarding traffic patterns and accidents. One academic researcher noted, however, that current data is relatively crude compared to the richness of sensory and internal data that connected cars may broadcast to nearby vehicles and infrastructure in real-time. Industry representatives stressed that for the full potential of these features to be realized, it is necessary to increase the number of connected cars on the road and eliminate unnecessary restrictions on the potential uses of such data.

Finally, privacy advocates noted that connected cars raise several novel questions that affect how privacy and security standards are applied. For example, who owns and is liable for data as it makes its way through various devices and databases? What protocols should exist for the storage or deletion of sensitive user information? And to what extent should manufacturers and dealers inform consumers about the features and risks of such technologies?

Cybersecurity Issues

The workshop's second panel featured cybersecurity experts from auto manufacturers, privacy advocates, and industry associations. Although panelists acknowledged that there is already a large degree of regulatory guidance and institutional knowledge around cybersecurity, most panelists agreed that connected cars present unique considerations, since connected cars have critical safety implications for drivers and others on the road.

From an engineering perspective, several panelists focused on the need to quickly detect and address vulnerabilities as they arise. One industry representative noted the inevitability of a cyber-attack, stating that "it's not if, it's when." Academic researchers and private sector experts alike agreed that no security network is foolproof, and, with enough time and resources, a vulnerability can be found within any system. One researcher even described how graduate students could hack into a car using a CD or a nearby Bluetooth device, which could pose a heightened danger because cars connect with an increasing number of external devices. **In this regard, privacy advocates noted that manufacturers should be vigilant about their methods of encryption and authentication and take care to actively address discovered vulnerabilities.**

Similarly, panelists appeared to agree that there is an inherent tradeoff between the convenience of a feature and the security of the system, but that companies should design products and services with privacy and security in mind, at least to the extent possible. One researcher explained that the same user-friendly technology that allows a car to be unlocked with a fingerprint or started with an app introduces security risks that are not present when a physical key is required. As connected cars become more complex and their internal components become centrally coordinated, security experts emphasized that it is becoming ever more important to design resilient security networks and increase the preparedness of cybersecurity teams to respond to a breach.

The panelists also discussed whether security updates to cars, whether remotely or through the dealerships, should become automatic or more incentivized. After all, as one industry representative pointed out, the advantages of connected cars are reduced if safety and security features are not routinely checked, a problem likened to the danger of not responding to a factory recall for defective airbags, but with farther-reaching consequences. Privacy advocates, in turn, disagreed about whether potential penalties for companies who fail to adequately protect data are either too harsh or not harsh enough. One privacy advocate noted that "this is a live ballgame" and that questions about cybersecurity standards ultimately will fall to enforcement agencies such as the FTC and NHTSA to decide in the future.

Privacy Issues

In the third and final panel, a wide range of stakeholders addressed privacy issues raised by connected cars. **All panelists appeared to recognize that consumers expect companies to be transparent about their data practices and to take steps to protect data.** A representative from the Association of Global Automakers noted that it and the Alliance of Automobile Manufacturers already published a set of Consumer Privacy Protection Principles for Vehicle Technologies and Services and implemented its Framework for Automotive Cybersecurity Best Practices. **However, privacy advocates argued that existing self-regulatory principles do not adequately address certain fair information practice principles ("FIPPs"), such as minimizing data collection or deleting data when it is no longer needed for its intended purpose.** In response, industry representatives stated that emerging technologies raise complex privacy issues and that stakeholders must constantly consider and update best practices to address such issues.

Some industry representatives recognized that there is room for regulatory and legislative guidance on what information can be collected, used, and shared with third parties, and potentially released to government authorities. Panelists noted that the traditional FIPPs may need to be uniquely applied to data collected through connected cars, especially given the sensitivity of the information collected and the potential benefits of collecting more information to improve safety. **A concern among privacy advocates, for example, was that the collection of behavioral data by insurance companies would be used to increase insurance rates. On the other hand, industry representatives were concerned that data on malfunctioning engine parts would be essential to suppliers and safety engineers, which makes the decision to give consumers autonomy over this data more difficult.** Privacy advocates also noted that the ability of law enforcement to track a stolen car or discreetly verify a suspect's alibi may be critical to an investigation, but access to such data may increase security vulnerabilities or reduce consumer trust in the technology as a whole.

Finally, privacy advocates raised concerns about the ability of companies to adequately protect consumer privacy when the data generated is highly individualized. Researchers on the panel stated that with so many unique data points being generated at once, the ease with which anonymized data can be "re-identified" increases no matter how much effort is put into de-identifying it. This may have an impact on consumers' choices about whether the safety and convenience of connected car features are worth the potential risks to privacy.

The Road Ahead: How Companies Can Stay within the Lane

The road ahead presents many privacy and security challenges for companies that collect, use, or share data through connected cars. The FTC/NHTSA workshop made it clear that the agencies are interested in developing and applying appropriate privacy and security standards to connected cars. As noted above, we expect the FTC Staff, alone or in combination with NHTSA Staff, to issue a report or other business guidance following the workshop and NHTSA to incorporate ideas from the workshop into its own rules, guidance, and interpretation of existing laws. In the meantime, companies can look to existing FTC guidance and self-regulatory principles and best practices, including the Consumer Privacy Protection Principles for Vehicle Technologies and Services and the Automotive Cybersecurity Best Practices.

It remains to be seen whether Congress will act separately to address privacy and cybersecurity standards for connected cars. Last month, in advance of a Senate Commerce Committee hearing titled "Paving the Way for Self-Driving Vehicles," several Senators called for legislation that "must address the connectivity of self-driving vehicles and potential cybersecurity vulnerabilities before they compromise safety." In addition, the House Digital Commerce and Consumer Protection Subcommittee recently held a hearing to discuss a wide range of self-driving vehicle legislation. At this time, however, legislative proposals to address privacy and cybersecurity standards for connected cars are still in the early stages.