wiley

NEWSLETTER

Connected Cars and a Deluge of Data

February 2019

Privacy in Focus®

Vehicles continue to become more connected – to each other, to surrounding infrastructure, to mobile devices, and to the cloud. New technologies such as 5G will enable faster connectivity and greater functionality. Cars will provide more customized user experiences, enhanced entertainment options, and seamless integration with other Internet of Things (IoT) services. And with this will come much, much more data being collected and shared. Indeed, some observers have projected that fully autonomous vehicles could eventually generate *terabytes* of data a day.

As the amount of data collected and shared increases, privacy and security regulatory concerns will be at the forefront. To date, the federal government has largely focused on best practices and industry self-regulation in the areas of privacy and data security in vehicles, rather than regulatory or enforcement actions. But both federal and state regulators have emphasized that privacy and data security enforcement will be priorities, and states in particular have ramped up their enforcement efforts in these areas.[1] And the history of the Federal Trade Commission's (FTC) approach to privacy and security in the area of mobile devices suggests greater scrutiny is coming, as vehicles ramp up and even surpass the amount of data collected and shared by mobile devices.

Federal Efforts to Date

Much of the attention on car connectivity to date has focused on adoption of vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications for the purposes of improving safety.[2] But regulators have acknowledged the potential privacy and security issues surrounding the collection and sharing of certain data, even

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Practice Areas

Connected & Autonomous Vehicles
Internet of Things
Privacy, Cyber & Data Governance

while avoiding proscriptive solutions. In mid-2017, for example, the National Highway Traffic Safety Administration (NHTSA) and the FTC held a joint workshop on privacy and security issues on connected cars. The FTC subsequently released a staff perspective summarizing the conference and potential issues on its radar.[3]

In general, the U.S. Department of Transportation has largely focused on safety concerns and conceded the policing of privacy issues to the FTC. Its late-2018 guidance on automated vehicles notes, for example, that DOT "takes consumer privacy seriously, diligently considers the privacy implications of our safety regulations and voluntary guidance, and works closely with the [FTC] ... to support the protection of consumer information and provide resources related to consumer privacy."[4]

Potential Privacy and Cybersecurity Issues

Connected vehicles can collect and share a wide range of data – and the potential legal issues can differ depending on the type of data. Notably, the industry has taken steps to adopt best practices in the privacy area. In 2014, the Alliance of Automobile Manufacturers and Association of Global Automakers jointly released Consumer Privacy Protection Principles for vehicle technologies and services.[5] These provide an important anchor as the legal and regulatory landscape around privacy protections continues to evolve. Some key areas of interest include:

Biometric data. Vehicles now have the technology to more closely monitor driver characteristics – for example, sensors that could detect distracted driving. Indeed, the Department of Transportation has suggested that companies are "encouraged to consider whether it is reasonable and appropriate to incorporate driver engagement monitoring in cases where drivers could be involved in the driving task so as to assess driver awareness and readiness to perform the full driving task."[6] Vehicles also can use facial recognition to provide the driver with augmented views or navigation systems.

Collection and use of biometric information can raise issues under some state laws – most notably the Illinois Biometric Information Privacy Act (BIPA), which requires notice and consent to use of certain biometric identifiers.[7] As detailed elsewhere in this issue, class action plaintiffs have been litigious in bringing claims under BIPA's private right of action, regardless of whether they can show that consumers were actually harmed by alleged violations. Additionally, FTC staff has noted that vehicles might collect fingerprints or iris patterns, which it views as "sensitive data" – which could suggest higher levels of scrutiny under the FTC's Section 5 authority.[8] The use of biometric data is certainly one area where the legal and regulatory outlook can move quickly, and that will need to be monitored.

Location data. Just as with phones, vehicles can collect detailed information about a person's whereabouts and activities. Some of this information can be used for safety purposes; as the FTC notes, manufacturers can collect "precise geolocation information to direct emergency personnel to the scene of a crash."[9] However, the sharing of location information has drawn congressional scrutiny in the context of mobile devices, with Members of Congress pushing for investigations into the sharing of such data with third parties. In this area, the manufacturers' Privacy Principles require affirmative consent for using geolocation information as the basis

for marketing or sharing that information with unaffiliated third parties for their own purposes, including marketing.[10] Companies involved in connected vehicles will want to carefully consider developments in this area.

Commercial data. Vehicles' infotainment systems may collect information about consumers' commercial activities or browsing activities, either by syncing with users' mobile devices or by collecting information though user interaction with the vehicle – such as by providing voice assistance or payment opportunities.[11] This information is potentially valuable to advertisers and can help tailor experiences for consumers. For example, a driver will be able to ask the vehicle's voice assistant for suggestions, and the responses could be tailored to the individual's transaction history.

While this kind of data collection is common on mobile devices, FTC staff has noted some skepticism, writing that "consumers may be concerned about secondary, unexpected uses of such data. For example, personal information about vehicle occupants using the vehicle's infotainment system, such as information about their browsing habits or app usage, could be sold to third parties, who may use the information to target products to consumers."[12] At the workshop, at least for information that was collected by syncing a mobile device, FTC staff's view was that there was a consensus on best practices 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."[13] Regulators' privacy concerns with mobile devices and infotainment systems may continue to converge as the two platforms increasingly become connected.

Driver behavior data. As the FTC notes, vehicles can collect "information about consumer driving habits, such as if a driver regularly speeds or slams on the breaks." CC at 2. Vehicles might collect such information for safety or operational reasons. The manufacturers' Privacy Principles currently require consent for sharing this kind of information with third parties, such as insurers, who use it for their own purposes,[14] and industry participants may run into more scrutiny if the information is shared outside of the context of safety and other limited purposes. FTC staff notes, for example, that one potential benefit of this data collection is that "consumers who demonstrate good driving habits can qualify for insurance discounts," but that "[s]ome participants viewed this use as a benefit rewarding safer driving; others were concerned about the potential for insurance companies to use this information, without consumers' knowledge, to raise rates, or to penalize safe drivers who choose not to authorize the collection of information."[15]

Cybersecurity. Advancements in connectivity and vehicle capability will make cars attractive targets for hackers. The security issues are not limited to hackers attempting to take control of the vehicle in some way; instead, hackers might attempt to access sensitive information that could be used for phishing attempts or other kinds of fraud. Connected vehicles can pose unique cybersecurity challenges. For one, the life cycle for vehicle systems is much longer than for other consumer products – cars typically stay on the road much longer than a consumer typically keeps a mobile phone. Connected vehicle systems need to be capable of being updated over time, including to address vulnerabilities that were not known at the time of manufacturing. And software patches and updates need to be pushed out on an ongoing basis, just as with PCs and mobile devices.

Industry participants are moving toward voluntary best practices and collaborative approaches on information-sharing to enhance cybersecurity across the industry. DOT has encouraged companies to incorporate industry practices on cybersecurity at the design state, and to "establish robust cyber incident response plans."[16] The Automotive Information Sharing and Analysis Center (Auto-ISAC) has, for example, released Automotive Cybersecurity Best Practices, covering governance, risk management, security by design, threat detection, incident response, training, and collaboration with appropriate third parties.[17] And both the FTC[18] and the DOT[19] have endorsed voluntary information sharing of cybersecurity threats through industry groups. These kinds of cybersecurity efforts will be critical as vehicles collect and generate increasing amounts of data and become targets.

Conclusion

The deluge of data generated and shared by vehicles will continue to grow, and policymakers and regulators will no doubt be grappling with how to treat different kinds of data and whether to take more proscriptive actions on privacy or data security. Industry participants have taken the lead in best practices but should remain well aware of how quickly technological developments can push privacy and security issues to the forefront. As has happened with mobile devices, the actions that industry participants are taking now to deal with consumer data will be no doubt be subject to scrutiny going forward.

---

[1] *See* Peter S. Hyun and Duane C. Pozza, "Expect Aggressive Consumer-Related Investigations from State AGs," *Corporate Counsel* (Jan. 4, 2019), available at https://www.wileyrein.com/newsroom-articles-Expect-Aggressive-Consumer-Related-Investigations-from-State-AGs.html.

[2] *See, e.g.*, Scott D. Delacourt, "Top 5 Takeaways from ITS America 2018 on the V2X Path Forward," WileyConnect, June 7, 2018, available at https://www.wileyconnect.com/home/2018/6/7/top-5-takeaways-from-its-america-2018-on-the-v2x-path-forward.

[3] FTC Staff, Connected Cars Workshop: Staff Perspective, January 2018, available at https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf ("FTC Staff Perspective").

[4] U.S. Department of Transportation, *Preparing for the Future of Transportation: Automated Vehicles 3.0*, at 19 (October 2018), available at https://www.transportation.gov/av/3 ("AV 3.0").

[5] The Consumer Privacy Protection Principles are available at https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.

[6] U.S. Department of Transportation, *Automated Driving Systems (ADS): A Vision for Safety 2.0*, at 10 (September 2017), available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf ("AV 2.0").

[7] 740 ILCS 14/1 *et seq*.

[8] FTC Staff Perspective at 2.

[9] *Id*.

[10] Consumer Privacy Protection Principles at 8.

[11] See Duane C. Pozza, "New Issues Raised by Internet of Things Payments," *Law360* (January 4, 2019), available at https://www.wileyrein.com/newsroom-articles-New-Issues-Raised-By-Internet-Of-Things-Payments.html.

[12] FTC Staff Perspective at 2.

[13] *Id*. at 3.

[14] Consumer Privacy Protection Principles at 8; *see also* Auto Alliance FAQ, https://autoalliance.org/connected-cars/automotive-privacy/#automotive-privacy/what-do-consumers-need-to-know-and-do-to-protect-their-vehicle-information-and-car-data-privacy.

[15] FTC Staff Perspective at 2.

[16] AV 2.0 at 11.

[17] *See* https://www.automotiveisac.com/best-practices/.

[18] FTC Staff Perspective at 3-4.

[19] AV 3.0 at 17-18.

© 2019 Wiley Rein LLP