Bloomberg Law®

bloombergbna.com

INSIGHT: Monitoring Mobility--The Current and Future Regulatory Landscape for Advanced Automotive Tech




By Jason Chipman, Reed Freeman, Todd Zubler and Allison Aviki

This is the fourth article in a series of five articles written by WilmerHale lawyers discussing how the emergence of IoT technologies will impact the automotive industry. The first article, ''The Developing Landscape of Internet of Things Standards for Cars,'' published on November 5, the second, ''Internet of Vehicles Technologies as Patentable Subject After Alice*,'' on November 20, and the third, ''What to Expect in Licensing and Litigation as the Internet of Things Comes to the Automotive Industry,'' on December 3.*

Monitoring Mobility

''Now the most advanced tech you own is in your driveway'' announces the closing line of a 2018 Nissan commercial. As cars have become synonymous with ''advanced tech,'' automakers have retooled and rebooted as tech-focused companies. Ford has become a mainstay at the annual CES, formerly known as the International Consumer Electronics Show, and automotive research facilities are serious operations in Silicon Valley. Consider the industries now deemed adjacent to automotive: chipmakers; wireless phone manufacturers; software developers; cloud storage services; advertisers; and the data security industry.

The proliferation of advanced tech in cars has pushed automakers and suppliers into uncharted territory in terms of the services they provide and the companies they must compete and cooperate with.

The automotive industry has historically been a highly regulated one, but the convergence of automotive and other advanced technologies has subjected car manufacturers and suppliers to a host of new laws, rules, best practices, and oversight. This article looks at updates in the regulatory space by reviewing major touchpoints for mapping automotive's future: autonomous driving; ride-sharing; and connectivity. We conclude with keys to navigating the regulatory landscape in 2018-2019.

Autonomous. The shift from current *driver-assist* technologies to *driverless* vehicles is well underway, with a majority of Americans now agreeing that the latter will be common within a decade, according to an April 2018 Gallup poll. On October 4, the Department of Transportation (''DOT'') released its own plan forward for automated cars, including its recognition that the term ''driver'' may ''not refer exclusively to a human'' but may instead ''include an automated system.'' DOT also affirmed that it ''will modernize or eliminate outdated regulations that unnecessarily impede the development of automated vehicles.'' Continuing the emphasis on deregulation, the National Highway Traffic Safety Administration (''NHTSA'') has earmarked $21.5 million in next year's budget for rulemaking programs designed to ''promote safety and innovation through effective use of . . . deregulation.''

At the same time that federal agencies are eyeing deregulation, both the House and the Senate have taken up efforts to pass national legislation. A key goal driving Congressional legislative efforts has been preempting the patchwork of state regulations that have cropped up in recent years. Despite early momentum, however, the SELF DRIVE Act and AV START Act—seen by backers and critics alike as concentrating at the federal level regulatory power over autonomous vehicle testing and deployment—have stalled in recent months. On October 5, chairman and CEO of General Motors Mary Barra published an opinion piece for Axios highlighting both bills and urging that ''[f]ederal legislation

would provide a path for manufacturers to put self-driving vehicles on the roads safely, while allowing continued innovation.'' As of this writing, however, there has been no recent action on these bills.

In the absence of federal legislation governing autonomous vehicles, states and localities are not hesitating to step into the breach. According to the National Conference of State Legislatures, there are 29 states with autonomous vehicle legislation in place. Many of these state rules—for example Michigan's SB 995—delineate the conditions by which autonomous vehicles may be operated on public roadways or, like Pennsylvania's SB 1267, authorize the allocation of public funds for autonomous-related development. Relatedly, multiple complementary executive orders have issued at the state level. Some, including Arizona Governor Doug Ducey, have used such orders to encourage expansive testing of autonomous vehicles.

Companies have reacted in kind. In December 2017, for example, a *USA Today* story titled ''Why automakers flock to Arizona to test driverless cars'' pointed to the state's ''relatively light regulatory environment.'' Several months later, the *New York Times* cited Arizona's ''lenient approach to regulation'' after a self-driving car struck and killed a pedestrian in Tempe.

Ride-Sharing. With automobile sales projected to decline while ride-sharing services proliferate and consumers buy fewer cars of their own, automakers are looking to expand their revenues by entering the ride-sharing market. BMW has launched ReachNow, a ride-hailing service with human drivers in Seattle. In January 2018, the *Detroit News* reported that General Motors is looking at an even more advanced option: GM filed a Safety Petition with NHTSA to deploy a driverless ride-hailing fleet.

By moving into the ride-sharing market, automakers are entering a sector that has been drawing sharp scrutiny on multiple fronts. Earlier this year, the CEOs of the most prominent ride-sharing companies received a letter from members of Congress after CNN reported on accusations of sexual assault of passengers by drivers. Questions included, ''In what instances does your company refer charges [by customers] to law enforcement and cooperate with their investigations?'' and whether the companies have ''a protocol in place to ensure other [ride-sharing] companies . . . are alerted to'' allegations given that drivers ''may be employed by multiple ridesharing companies.''

Lyft and other ride-sharing companies have also faced recent private enforcement actions in various states brought by disability rights groups citing anti-discrimination laws that require taxi and bus services to provide accommodations to riders with disabilities.

In August 2018, the New York City Council attracted widespread media coverage for passing legislation capping the number of ride-sharing vehicles permissible on roadways. As Wired reported, in an effort to address traffic congestion and in recognition of a series of tragic suicides by taxi drivers, the City plans a one-year freeze on the total number of licenses available to companies and also sets a minimum wage for drivers. Non-compliance can lead to stiff fines.

Connectivity. Collecting data on drivers is nothing new. Progressive launched Snapshot—individualized insurance rates based on data collected about an individual's driving habits—all the way back in 1998. Now many major insurers offer benefits for drivers voluntarily sharing their driving data. But with the explosion of connectivity in automobiles, the possibilities for data collection have scaled to previously-unforeseeable levels. One SAS white paper estimates that, by 2020, a single car will produce 30 *terabytes* of data daily.

Automakers are suddenly learning more about drivers (and passengers) than previously imaginable, from precise location data, to biometric and health data, to infotainment preferences. For example, companies such as Telenav Inc. are developing an ''In-Car Advertising Platform'' that enables location-based mobile advertising. And while the concept of biometric vehicle access (think starting your ignition with a retina scan) is nothing new, in-car technology capable of monitoring everything from driver heart rate to brain waves is underway.

Whether through onboard interfaces, mobile interoperability, or under-the-hood data collection, the possibilities for how and when consumer data are collected, used, monetized, or otherwise disclosed are increasing every day. As Gabrielle Coppola and David Welch wrote in Bloomberg Businessweek earlier this year, ''[T]he big question for automakers now is whether they can profit off all the driver data they're capable of collecting without alienating consumers or risking backlash from Washington.''

In such an environment, automakers will necessarily collaborate with third-party developers. On the 150th anniversary of Henry Ford's birth, for example, Ford Motor Company launched ''Ford Dev,'' the company's developer program for in-car applications. Examples abound of tech companies that have similarly tried, with both successes and failures, to foster healthy independent development ecosystems.

Such far-ranging information has the potential to invoke an equally far-ranging spectrum of issues, from anti-wiretapping laws, to HIPAA compliance, to GDPR and California's Online Privacy Protection Act, and, of course, privacy and data security provisions under Section 5 of the Federal Trade Commission Act.

During summer 2017, the Federal Trade Commission (FTC) partnered with NHTSA to host a daylong ''Connected Cars Workshop,'' bringing together stakeholders ranging from academia, to advocacy groups, to government and industry in order to assess consumer privacy and security issues raised by cars that are connected to the internet. The issues highlighted by the ''Staff Perspective'' on the workshop included the need for transparency regarding the collection of information that is not critical for safety; data sharing with third parties, including insurance companies; whether and how data will be aggregated and anonymized; the potential for the collection of biometric information, which the FTC considers sensitive; and the need to secure all of the data collected by connected cars.

The Alliance of Automobile Manufacturers and Global Automakers has previously embraced self-regulatory guidelines contained in the 2014 Automotive Consumer Privacy Protection Principles. These principles staked out various commitments: transparency about collection practices; data minimization efforts; and consent-driven schemes that serve as a gating mechanism to third-party sharing. In a positive sign for participating automakers, the principles generally align with the ''approach to consumer data privacy'' that the federal National Telecommunications and Information

Administration announced in September 2018. Additional new resources include the ''Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks'' by the National Institute of Standards and Technology (''NIST''), also published September 2018, and the nonprofit Future of Privacy Forum's aggregated writing on connected cars.

Regulatory efforts, however, will likely extend beyond self-regulation. NHTSA has announced that it agrees with the recommendation of the Government Accountability Office that NHTSA should ''define, document, and externally communicate its roles and responsibilities related to the privacy of data generated by and collected from vehicles.'' The FTC, meanwhile, is already a familiar government stakeholder in the consumer privacy and data security spaces, and more oversight by the FTC should be expected. In addition, state Attorneys General frequently and aggressively bring actions against companies accused of violating their respective state data breach laws.

Finally, the new connectivity of cars creates not only privacy concerns but also significant and growing cybersecurity risks. In 2015, Fiat Chrysler recalled 1.4 million cars after two researchers published a *Wired* article demonstrating their ability to remotely hack control of a Jeep Cherokee. NHTSA opened an investigation and shortly thereafter published ''Cybersecurity Best Practices for Modern Vehicles.'' The incident helped spur serious attention to vehicle cybersecurity and led to industry stakeholders collaborating on information-sharing and threat-tracking. Notably, the Automotive Information Sharing and Analysis Center (''Auto-ISAC'') recently held its second annual conference. The group continues to expand its membership ranks among automakers and suppliers, which will promote collaborative efforts to prevent, identify, and police cybersecurity threats.

Keys to Navigating 2018-2019. 1. **Privacy:** Consumers and representative groups are monitoring companies to ensure they provide transparency, minimization, de-identification, data security, and consumer control over their data. So know the answers to the following questions.

a. ***Automakers***: What consumer data is your company collecting? Are you sharing that data with anyone, deliberately or not? Are you collecting data for internal use for safety, or for other reasons? If for other reasons, such as advertising or sale to insurance companies, how do you make sure consumers are aware of this? How can consumers opt out? Have you ensured that consumer data is collected and shared transparently, in compliance with your privacy policy and other privacy-related statements, and do you provide consumers with choice regarding your use and sharing of the data your vehicles collect, and take care that you don't use the data unlawfully, such as by violating antidiscrimination laws at the federal and state levels?

b. ***Third Parties such as app developers and other third-party data collectors/recipients***: Anticipate being asked the questions above and collaborate with automakers to answer those questions on the front end, not when it is already too late.

2. **Data Security**: With cars becoming a large and complex device connected to a larger, wired world, manufacturers are increasingly expected to design secure devices that can operate safely and efficiently despite global cyber threats. Providing reasonable security (as described by the FTC in a 2015 report and in a related blog series) of the information collected and accessible through automotive systems is critical. Automakers and developers should design security features into their connected cars and test their security on a regular basis. They also should stay in conversation with others in the automotive and high-tech spaces, particularly now that public/private partnerships to share threat intelligence are strengthening. Moreover, state regulations matter, particularly substantive data security laws, such as the now well-tested state data breach laws and Massachusetts' 201 CMR 17: Standards for the protection of personal information of residents of the Commonwealth. Don't let the first test of your compliance protocol for your connected cars be the day a breach is discovered.

The fifth and final article of this series will discuss the future of automotive trade secret litigation and will publish next week.

D. Reed Freeman, Jr. is a partner at WilmerHale. He is a leading authority on privacy, cybersecurity, and online, mobile, and social media advertising and privacy law. Mr. Freeman serves as co-chair of the firm's Cybersecurity, Privacy and Communications Practice. He can be reached at reed.freeman@wilmerhale.com.

Jason Chipman is a partner at WilmerHale. He is widely recognized as a national leader in handling complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States (CFIUS) and related export controls. Mr. Chipman can be reached at jason.chipman@wilmerhale.com.

Todd Zubler is a partner at WilmerHale. His practice focuses on civil litigation, with a particular emphasis on intellectual property and appellate litigation. Mr. Zubler can be reached at todd.zubler@wilmerhale.com

Allison Aviki is a senior associate at WilmerHale. She focuses her practice on intellectual property litigation at the trial and appellate level. Ms. Aviki can be reached at allison.aviki@wilmerhale.com.