NHTSA'S CLAIMED JURISDICTION OVER SOFTWARE AND APPLICATIONS MAY STIFLE INNOVATION

Date: 14 April 2016

Telecom, Media and Technology Alert

By: Cliff L. Rothenstein, Thomas R. DeCesar, Edward J. Fishman, Robert A. Lawton

Motor vehicle technology is rapidly changing to enhance safety and provide navigation, mobility, and accessibility solutions for drivers. Manufacturer-installed automatic braking, adaptive cruise control, blind-spot monitoring, and lane departure warnings are becoming common in new passenger cars. Software developers have created smartphone applications that provide directions, pay tolls, warn drivers of traffic and speed traps, or simply give information about where to eat. Other applications prevent distracted driving by locking-out or simplifying smartphone functions. Car connectivity also is on the rise through manufacturer-installed and aftermarket devices. On the horizon, many industry experts predict that self-driving car technology will be ready for widespread public use in the next five to ten years. This is an exciting time for innovation in the motor vehicle industry.

Against this background, the National Highway and Traffic Safety Administration ("NHTSA") issued a draft Enforcement Guidance Bulletin on April 1, 2016, in which it announced that it has interpreted its jurisdiction under the National Traffic and Motor Vehicle Safety Act ("Safety Act") with regard to emerging motor vehicle technologies.[1] Comments in response to NHTSA's bulletin are due by May 2, 2016. Under its draft interpretation, NHTSA claims its authority under the Safety Act extends to:

> (1) automated vehicle technologies, systems, and equipment, whether sold as part of a new motor vehicle or as an aftermarket replacement or improvement; and (2) software, such as mobile apps (including programs, instructions, code, and data), and after-market software updates. This could also extend to software that enables devices, which are not located in or on the vehicle, to connect to the vehicle.

NHTSA's jurisdiction over "motor vehicle equipment" is based on the definition of the term in Section 30102(a)(7) of the Safety Act. This section provides that motor vehicle equipment includes:

> (A) any system, part, or component of a motor vehicle as originally manufactured; (B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or (C) any device or an article or apparel . . . that — [] is not a system, part, or component of a motor vehicle[] and [] is manufactured, sold, delivered . . . with the

> apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death.[2]

In short, under the Safety Act, NHTSA's authority over motor vehicle equipment covers the parts that comprise a motor vehicle (whether original or replacement), accessories and additions to motor vehicles, and motor vehicle safety devices and apparel.

Accordingly, with regard to new automated vehicle technologies, systems, and equipment, whether sold as an aftermarket part or integrated into a new motor vehicle, NHTSA's pronouncement is entirely conventional. The fact that equipment is new or emerging does not affect the scope of the Safety Act. NHTSA's jurisdiction under the Safety Act extends to motor vehicle equipment that automatically stops a car before a collision, in the same way that its jurisdiction extends to anti-lock brake systems or automatic windows. These are all motor vehicle systems, parts, or components, even if they are emerging technologies or have electrical components.[3]

This matter was not in doubt. So why did NHTSA expend the effort of publishing the draft bulletin to address it? NHTSA wanted an opportunity to announce its claimed jurisdiction over software — specifically apps for mobile devices. Other than NHTSA's claim regarding its alleged jurisdiction over software, the agency's bulletin was largely unnecessary.

By claiming that its jurisdiction extends to software, including associated programs, instructions, code, and data, NHTSA has significantly expanded the scope of the Safety Act to incorporate items that ***are not*** motor vehicle systems, parts, or components. Software/apps are a different kind of animal than anything that NHTSA has regulated in the past — the agency has historically concentrated on the physical components of motor vehicles, as provided under the Safety Act. Moreover, NHTSA now claims the Safety Act also extends to software that is not even in a car, but that can affect the car through a remote connection. Given this background, it is not surprising that the agency fails to cite any statutory support or precedent to explain why it believes that its jurisdiction under the Safety Act extends to software/apps.

An illustration is helpful to understand what NHTSA is attempting to do in the draft bulletin. NHTSA undoubtedly has authority over a car's radio — to either require a recall if there is a safety defect in the radio (*e.g.*, the radio causes a fire after prolonged use) or to promulgate regulations requiring radios to meet certain specifications (*e.g.*, radios must remain under a certain decibel level). NHTSA has the authority in this area because car radios are motor vehicles parts. In its recent pronouncement, however, NHTSA has essentially determined that it not only has authority over the radio, but also the signal travelling to the radio and the computer program and equipment transmitting that signal. NHTSA's bulletin signals the agency's shift away from its clear authority over motor vehicle parts to the amorphous world of items (including software and applications) affecting motor vehicle parts or the motor vehicle itself. Unfortunately for the agency, its position is not supported by the express language of the Safety Act.

Moreover, while NHTSA claims its bulletin is for enforcement guidance and informational purposes only, the implications of the bulletin could significantly affect software developers creating and offering applications that can be used in conjunction with a motor vehicle or that can be used in cars through a remote connection. These developers may unexpectedly face significant NHTSA recall obligations based on errors or defects in their products. From a cybersecurity perspective, app developers may need to start evaluating hacking and infiltration vulnerabilities from a defect and recall perspective. If NHTSA believes it necessary, the agency may utilize its

investigative and civil enforcement authority (including the imposition of civil penalties) with regard to software and apps that it believes pose a safety risk. Lastly, in the future, the agency could promulgate regulations affecting software and apps under its new interpretation of the Safety Act.

In the end, NHTSA's unsupported pronouncement may end up stifling innovation and making software development companies think twice before developing or offering software for drivers and the motor vehicle industry, effectively hindering the development of emerging motor vehicle technology. Companies concerned with NHTSA's expansive view of its own jurisdiction should consider filing comments in response to the agency's bulletin prior to the May 2, 2016 deadline.

Notes:

[1] Safety-Related Defects and Emerging Automotive Technologies, 81 Fed. Reg. 18935 (Apr. 1, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-04-01/pdf/2016-07353.pdf.

[2] 49 U.S.C. § 30102(a)(7).

[3] *Id.*

KEY CONTACTS

CLIFF L. ROTHENSTEIN
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON DC
+1.202.778.9381
CLIFF.ROTHENSTEIN@KLGATES.COM

THOMAS R. DECESAR
PARTNER

HARRISBURG
+1.717.231.4563
THOMAS.DECESAR@KLGATES.COM

