CLIENT ALERT

NHTSA Addresses Hacking and Cybersecurity

Jun.01.2016

The National Highway Traffic Safety Administration (NHTSA) issued two publications focused on emerging vehicle technologies and associated risks. In mid-March, NHTSA and the Federal Bureau of Investigation (FBI) cautioned the public about hacking risks. In April, NHTSA requested public comment on its assertion that emerging technologies are subject to NHTSA's existing enforcement authority.

On March 17, 2016, NHTSA and the FBI jointly released a Public Service Announcement (PSA) about risks of vehicle hacking. The PSA, which is directed to the general public as well as manufacturers of vehicles, vehicle components and aftermarket devices, defines "vehicle hacking" as "someone with a computer seek[ing] to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality." The PSA identifies ways in which modern technologies expose vehicles to hacking threats and describes how "attackers" may access vehicle networks and driver data.

The PSA acknowledges that "not all hacking incidents may result in a risk to safety," but warns consumers to recognize vulnerabilities that their vehicles may face, and to take precautions against them. The report encourages consumers to ensure that their vehicles' software is current, that they do not make unauthorized modifications to vehicle software, that they exercise discretion when connecting third-party devices (like cell phones and insurance dongles) to their vehicles, and that they be aware of who has physical access to their vehicles.

The PSA does not ask the automotive industry to take similar precautionary steps and does not criticize current industry efforts to expand cyber security measures. To the contrary, it highlights that the automotive industry has established an Information Sharing and Analysis Center to exchange cyber security information, and is collaborating to develop best practices for enhancing vehicle cyber security. The PSA also reports that NHTSA is "actively working on several initiatives to improve the cyber security posture of vehicles in the United States."

On April 1, NHTSA issued a Request for Public Comments on NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Emerging Automotive Technologies. Unlike its PSA on hacking, this notice focuses squarely on manufacturer obligations. The bulletin sets forth NHTSA's position that its "enforcement authority concerning safety-related defects in motor vehicles and equipment extends and applies equally to new and emerging automotive technologies," including software. Comments to the bulletin were due to NHTSA by May 2, 2016.

The majority of the bulletin reiterates NHTSA's position on how manufacturers should determine whether a defect exists and whether a defect presents an unreasonable risk to safety. The bulletin also identifies best practices for ensuring that manufacturers of emerging technologies comply with the National Traffic and Motor Vehicle Safety Act. The bulletin recognizes that manufacturers should have autonomy in determining and implementing best practices, which may vary depending upon the circumstances, and NHTSA identifies a non-exhaustive list of factors that it will weigh when determining whether a cybersecurity vulnerability poses an unreasonable risk to safety:

i. Amount of time elapsed since the vulnerability was discovered.
ii. Level of expertise needed to exploit the vulnerability.
iii. Accessibility of knowledge of the underlying system.
iv. Necessary window of opportunity to exploit the vulnerability.
v. Level of equipment needed to exploit the vulnerability.

The bulletin explains that NHTSA may increase the weight it gives to the probability of an attack when there are confirmed incidents of the vulnerability being exploited in a malicious cybersecurity attack. Further, a cybersecurity vulnerability in a vehicle's entry points (*e.g.*, Wi-Fi, infotainment systems, the OBD-II port) that allow remote access to critical safety systems may be "a safety-related defect compelling a recall."

In the bulletin, NHTSA encourages manufacturers to adopt a lifecycle approach to managing safety risks by considering "elements of assessment, design, implementation, and operations as well as an effective testing and certification program." The bulletin concludes by reminding "[m]anufacturers of emerging technologies and the motor vehicles on which such technology is installed [that they] have a continuing obligation to proactively identify safety concerns and mitigate the risks of harm." These later stages of the life cycle can provide some of the toughest challenges for manufacturers since they need to anticipate ways to monitor products that may change as they add new functionalities and applications over time.

While not all cybersecurity vulnerabilities present a defect or risk to safety, manufacturers need to be considering these issues moving forward.

Other Articles in This Month's Edition:

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Cheryl A. Falvey
Partner – Washington, D.C.
Phone: +1 202.624.2675
Email: cfalvey@crowell.com

Rebecca Baden Chaney
Partner – Washington, D.C.

Phone: +1 202.624.2772
Email: rchaney@crowell.com