crowell moring

CLIENT ALERT

Proposed Updates to the Motor Vehicle Safety Act

October 2015

On Wednesday, October 21, 2015, a U.S. House of Representatives subcommittee debated a draft bill that seeks to amend the National Traffic and Motor Vehicle Safety Act, 49 U.S.C. §§ 30101, *et seq*., "[t]o provide greater transparency, accountability, and safety authority to the National Highway Traffic Safety Administration [NHTSA], and for other purposes." The bill, which has drawn negative comments from NHTSA's administrator, the Federal Trade Commission (FTC), and some Democratic lawmakers, addresses a variety of vehicle safety matters, many of which are focused on emerging technologies and protecting consumer data. Issues include vehicle data privacy, cybersecurity and advanced automotive technologies.

Vehicle Data Privacy

If enacted, Title III of the draft bill would require each motor vehicle manufacturer to "develop and implement a privacy policy outlining" its practices "regarding the collection, use, and sharing of covered information." "Covered information" is information that a motor vehicle "collect[s], generate[s], record[s], or store[s] in electronic form," and information that a vehicle owner, lessee, or renter provides while using vehicle technologies that are provided or offered by or on behalf of the manufacturer and that access motor vehicle information..

The privacy policy must state whether the manufacturer provides vehicle users with:

- Notice regarding the collection, use, and sharing of covered information;
- Choices available to the user concerning collection, use, and sharing of covered information;
- An explanation of "[h]ow and under what circumstances covered information is collected";
- A commitment to retain covered information only for so long as is required for legitimate business purposes;
- A commitment to implement reasonable measures to protect covered information;
- A commitment to implement reasonable measures to maintain the accuracy of covered information, including mechanisms for vehicle users to review and correct such information;
- A commitment to take reasonable steps to ensure that the manufacturer and other entities that receive the information adhere to the policy.

Once developed, the manufacturer must file its privacy policy, and updates, with NHTSA, which will in turn publicly post the privacy policy and revisions.

A manufacturer that fails to submit a privacy policy or that violates its own policy is subject to a civil penalty of up to $5,000 per day, with a maximum penalty of $1,000,000. Under the draft bill, however, manufacturers whose privacy policy contains all of the required elements are exempt not only from the penalty provision but also from FTC enforcement actions under section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, "with respect to any unfair or deceptive act or practice relating to privacy."

The proposed data privacy provisions would also make all forms of vehicle "hacking"—malicious and otherwise —unlawful. More specifically, it would be unlawful for "any person to access, without authorization, an electronic control unit or critical system[1] of a motor vehicle, or other system containing driving data for such motor vehicle, either wirelessly or through a wired connection." A person who violates this provision is liable for a civil penalty not to exceed $100,000 per violation.

Cybersecurity

The proposed bill would require NHTSA to establish an Automotive Cybersecurity Council comprising the NHTSA Administrator; at least one representative each from the Department of Defense, NIST, and NHTSA; and representatives from each vehicle manufacturer that sold more than 20,000 vehicles in the U.S. in the previous calendar year. NHTSA's Administrator would also have to appoint representatives from franchised car dealerships, independent repair shops, consumer advocates, parts suppliers, standards-setting bodies, academics, and security researchers. At least 50 percent of the final Council membership must be representatives of vehicle manufacturers.

The Council would meet at least quarterly to develop "cybersecurity best practices" for vehicle manufacturers, and then meet annually once those best practices are in place to review and update them as needed. The best practices may include, among others:

- The quality of security controls;
- The design of vehicle architecture with respect to connections between vehicle systems and critical safety systems;
- Security specifications imposed upon suppliers;
- Security controls around openings into vehicle networks and operating systems;
- "[R]emediation of cybersecurity vulnerabilities"; and
- Sharing cyber security vulnerability information with vehicle manufacturers and security researchers.

Once published, manufacturers have the option of confidentially submitting their vehicle security and integrity plans to NHTSA's Administrator for approval. If NHTSA does not deem the plan to comply with the adopted best practices, NHTSA will order the manufacturer to modify the plan. The plans would be exempt from public disclosure under the Freedom of Information Act, and manufacturers that implement and maintain NHTSA-approved plans will be exempt from FTC enforcement actions under section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, "with respect to any unfair or deceptive act or practice relating to the best practices the manufacturer implements and maintains[.]" In addition to creating incentives to comply with the best practices, the draft bill also makes clear that the best practices do not provide an independent basis for liability against manufacturers that do not implement them: "[t]he best practices issued by the Council … may not provide a basis for or evidence of liability in an action against a manufacturer of automobiles whose cyber security practices are alleged to be inconsistent with the best practices … if (A) the manufacturer has not filed a vehicle security and integrity plan [with NHTSA]; or (B) the plan of the manufacturer does not include the cyber security practice at issue."

Advanced Automotive Technologies

Under Title V of the proposed bill, the Secretary of Transportation would establish an "Advanced Automotive Technology Advisory Committee … to develop safety performance metrics for advanced automotive technologies and connected vehicle

technologies originally installed in motor vehicles." The bill defines "advanced automotive technology" as "any vehicle information system, unit, device, or technology that meets any applicable performance metric and demonstrates crash avoidance or congestion mitigation benefits," including technologies such as accident warning and avoidance systems, assisted and emergency braking, and applications to keep drivers in the appropriate lane, monitor their awareness, and provide similar driver support.

The Committee would develop safety metrics for advanced automotive or connected vehicle technology installed as original equipment in at least 15 percent of vehicles in a manufacturer's U.S. fleet and also develop test procedures for each technology. The Committee comprises the NHTSA Administrator, U.S. vehicle manufacturer representatives, representatives from standard-setting bodies, and other members as determined necessary. This section of the bill would also impose labeling requirements concerning such technologies, and would allow fuel economy credits for vehicles that include a certain number of advanced automotive technologies.

Additional Proposed Revisions and Additions

There are a number of additional revisions to the Safety Act in the proposed bill. Some of the more notable proposals include the following:

- Required improvements to the availability of safety recall information, including through a revised NHTSA website;
- Improved recall notification by requiring and/or allowing notification via e-mail, in addition to U.S. mail, and an audit of NHTSA's management of motor vehicle safety recalls;
- Implementing recall notifications upon registration of affected vehicles at the state level;
- Exemptions from compliance with certain Safety Act requirements for vehicles introduced into commerce for the purposes of testing or evaluation, if certain other criteria are met; and
- Limitations on liability asserted on the basis of NHTSA motor vehicle safety guidelines.

[1] This refers to "software, firmware, or hardware located within or on a motor vehicle that, if accessed without authorization, can affect the movement of the vehicle."

Other Articles in This Month's Edition:

- Transfer of Personal Data from the EU to the U.S.
- A Highlight Reel: FTC's Amendment to Fair Packaging and Labeling Act Rules
- Advertisers in the Ring – A Roundup of This Month's Competitor Advertising Challenges: Measuring '#1' and 'Free' Claims

---

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

Daniel T. Campbell
Partner – Washington, D.C.

Phone: +1 202.624.2544
Email: dcampbell@crowell.com

Rebecca Baden Chaney
Partner – Washington, D.C.
Phone: +1 202.624.2772
Email: rchaney@crowell.com