Crowell

Client Alert

Senator Markey Introduces the SPY Car Act to Regulate Automotive Cybersecurity

August 2015

On July 14, Senators Edward J. Markey (D-Mass) and Richard Blumenthal (D-Conn) introduced the Security and Privacy in Your Car Act of 2015, or "SPY Car Act." The bill, which would amend both the Motor Vehicle Safety Act (49 U.S.C. § 30101, *et seq.*) and the Federal Trade Commission Act (15 U.S.C. § 41 *et seq.*), has two purposes: (1) to create more secure vehicles, and (2) to better inform consumers about vehicle cybersecurity and the use of driving data.

The SPY Car Act seeks to achieve these goals by imposing both cybersecurity and labeling requirements on automotive manufacturers and by limiting the use of personal driving data. Specifically, if the bill were to pass in its current form, it would:

- **Require Federal Cybersecurity Standards for Vehicles:** The bill establishes three categories of cybersecurity standards for vehicles—anti-hacking, data security, and threat detection.
    - *Anti-hacking:* anti-hacking measures must be in place for all "entry points[1] to electronic systems." Further, manufacturers must incorporate "isolation measures" to separate "critical software systems," which affect the driver's control of vehicle movement, from non-critical software systems. These anti-hacking measures must also be evaluated for vulnerabilities, including through penetration testing, and adjusted and updated accordingly.
    - *Data security:* all driving data collected by electronic systems must be "reasonably secured" against unauthorized access.
    - *Threat detection:* any vehicle with an "entry point" must be able to "immediately detect, report, and stop attempts to intercept driving data or control the vehicle."
- **Establish Uniform Cybersecurity Labels for Vehicles:** The SPY Car Act would add a "cyber dashboard" to the mandatory fuel economy label to inform consumers about the extent to which the vehicle provides cybersecurity and privacy protection. This dashboard must be "easy-to-understand" and "standardized."
- **Limit the Use of Personal Driving Data:** The Act would amend the Federal Trade Commission Act to give the FTC authority to enforce privacy standards for motor vehicles and limit the use of personal driving data. All vehicles would have to provide "clear conspicuous notice, in clear and plain language" about the collection, transmission, retention and use of driving data. In addition, owners and lessees would have to be given the opportunity to terminate collection and retention of that data, and termination should not result in the loss of navigation or other features "to the extent technically possible." Finally, information collected by a motor vehicle could not be used for advertising and marketing purposes absent the consumer's express consent.

The SPY Car Act proposes that these requirements apply to all motor vehicles manufactured for sale in the United States two years after implementing regulations are enacted. Final regulations, per the SPY Car Act,

would be in place three years after it is enacted. Thus, these requirements could take effect in approximately five years. In addition, the regulations would be reviewed and updated every three years.

The SPY Car Act is one of several recent signals that Congress's interest in the Internet of Things is heightening. One of the bill's sponsors, Senator Markey, has been a particularly vocal advocate of increased regulation in this space. In February of this year, he released a report titled, "Tracking and Hacking: Security & Privacy Gaps that Put American Drivers at Risk." Also in February, Senator Markey proposed federal automotive cybersecurity standards at the Senate Committee on Commerce, Science, and Transportation hearing examining the Internet of Things. Senator Deb Fischer (R-NE) and Representative Leonard Lance (R-NJ) have likewise introduced and passed resolutions in the Senate and House seeking to impose a national strategy for the Internet of Things to promote economic growth and consumer empowerment.

Manufacturers, marketers, and others should follow Congressional activity on these issues closely, as this is likely just the beginning of increasing federal interest and action in this space.

---

[1] The Act defines "entry points" to include means by which "driving data" may be accessed or control signals may be sent or received. "Driving data" includes information about a vehicle's status (such as its location or speed) or its owners/operators/passengers.

Other Articles in This Month's Edition:

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

Clifford J. Zatz
Partner – Washington, D.C.
Phone: +1.202.624.2810
Email: czatz@crowell.com

Rebecca Baden Chaney

Partner – Washington, D.C.
Phone: +1.202.624.2772
Email: rchaney@crowell.com