The SPY Car Act of 2015: A first step in addressing cybersecurity threats to vehicles

Over the past 18 months, Americans have been bombarded with nearly non-stop news that yet another retailer, insurer, bank, hotel group, federal agency, or other entity has suffered a security breach achieved through unauthorized access to the victim’s network via the Internet. In the shadow of these (as well as other well-publicized “point of sale” credit card data theft) schemes, the potential threats to the security and privacy of users of Internet-connected devices, commonly referred to as the “Internet of Things,” or “IoT,” have not received as much acknowledgment or attention. Everything from home appliances, to fitness trackers, to medical devices that are implanted in humans, to the vehicles in which we travel, increasingly are designed and manufactured so that they can connect to the Internet. By one estimate, there will be 25 billion connected devices in operation by the end of 2015 and 50 billion by 2020.1 But along with the convenience and benefits that these products offer come threats to the safety and security of the users of the devices. For example, as has been recognized with respect to medical devices:

\[N\]etworked medical devices face the same technological vulnerabilities as any other networked technology. Hacktivists, thieves, spies, and even terrorists seek to exploit vulnerabilities in information technologies (IT) to commit crimes and cause havoc. However, when a networked device is literally plugged into a person, the consequences of cybercrime committed via that device might be particularly personal and threatening.2

The same holds true for the airplanes and cars in which millions of Americans travel every day for work and pleasure. Earlier this year, cybersecurity consultant Chris Roberts claimed to have penetrated the in-flight security of commercial airliners and taken over certain controls of between 15 and 20 flights between 2011 and 2014.3 And just this week, in a frightening but fascinating demonstration, Wired posted an online video showing how an Internet-connected private vehicle’s controls could be hijacked, with the driver powerless to stop the attack or control the vehicle, putting the safety of the driver, and others, at the mercy of the hackers.4

For several years, there have been calls for the federal government to pass comprehensive legislation to address cybersecurity threats to our safety and privacy, but so far, legislation, whether comprehensive or more limited, largely has failed to materialize. Now, that may be changing. On July 21, Senators Edward Markey and Richard Blumenthal took a step forward in the direction of protecting Americans against cybersecurity threats, at least in the area of the security and safety of passenger vehicles, by introducing S.1806, the “Security and Privacy in Your Car Act of 2015,” known by the short title, “SPY Car Act of 2015.” The introduction of this legislation comes five months after Senator Markey’s office highlighted potential security and privacy threats to connected vehicles in a report prepared by his staff.5 The SPY Car Act seeks to achieve its goal of “protect[ing] consumers from security and privacy threats to their motor vehicles” within the existing regulatory framework of two federal agencies, the National Highway Transportation Safety Administration (NHTSA) and the Federal Trade Commission (FTC). The three broad areas of proposed regulation are described below.
NHTSA “Cybersecurity Standards”
The centerpiece of the bill is a new “Cybersecurity Standards” provision that would be codified as 49 U.S.C. § 30129. The bill would require NHTSA, in consultation with the FTC, to issue a Notice of Proposed Rulemaking within 18 months after enactment of the legislation, and then to promulgate final regulations within another 18 months. The resulting Cybersecurity Standards would then take effect two years after the final regulations are promulgated, and would require all motor vehicles manufactured for sale in the United States to comply with standards in three broad areas:

Protection against “hacking”
• This would require that all “entry points” to the electronic systems of motor vehicles manufactured for sale in the U.S. be equipped with “reasonable measures” to protect against unauthorized access, by wired or wireless means, to electronic controls of the vehicle or “driving data.” Driving data is defined as electronic information “collected about . . . a vehicle’s status,” such as its location and speed, and “any owner, lessee, driver or passenger of a vehicle.”

• The “hacking” standard would further require “isolation measures” to separate “critical software systems”—defined as “software systems that can affect the driver’s control of the vehicle movement”—from “noncritical software systems.”

• The proposed legislation would also require these “hacking” prevention and “isolation measures” to be “evaluated for security vulnerabilities following best security practices,” including by penetration testing and other appropriate measures, and then updated or adjusted based on the results of the evaluation.

Security of collected information
• All “driving data” collected by the vehicle’s electronic systems must be “reasonably secured” to prevent unauthorized access while the data are stored on-board the vehicle, are in transit from the vehicle to another location (presumably, to the manufacturer or some other cloud-based service or location), or in any subsequent off-board storage or use.

Detection, reporting, and responding
• Any motor vehicle with an “entry point” must have the capability to “immediately detect, report, and stop attempts to intercept driving data or to control the vehicle.”

NHTSA “Cyber Dashboard”
A second aspect of the proposed legislation is the addition of a “Cyber Dashboard” component to the existing labeling requirements under 49 U.S.C. § 32908(b), which prescribes the contents of the “window sticker” that must be displayed by new car dealers on each vehicle. The “Cyber Dashboard,” as currently proposed, must include information to “inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements set forth in” the new Cybersecurity Standards of 49 U.S.C. § 30129 and the new “privacy standards” of the FTC Act, described below. As with the Cybersecurity Standards, NHTSA, in consultation with the FTC, must issue a proposed rulemaking within 18 months of the enactment of the legislation and promulgate final “Cyber Dashboard” regulations within another 18 months (or three years after enactment of the statute). Within two years of the final regulations, all motor vehicles manufactured for sale in the U.S. must display the “Cyber Dashboard” on the window sticker.

FTC “Privacy Standards”
In addition to the regulatory requirements administered by NHTSA, the SPY Car Act imposes limitations through a new provision to be added to the FTC Act (inserted after 15 U.S.C. § 57c-2), on the information that manufacturers may collect and retain about the owners or lessees of vehicles. The provision further mandates specific disclosures that must be provided about the information that is collected and retained. More specifically, the Privacy Standards include:

• a “Transparency” provision requiring each vehicle to “provide clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from the vehicle”;

• a requirement that the owner or lessee have the option to terminate the collection and retention of driving data, without losing access to navigation tools or other features or capabilities, “to the extent technically feasible”;
• an exception to the termination option in the case of driving data that is “required for post-incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs”; and

• a provision prohibiting manufacturers from using information collected by the vehicle for advertising or marketing purposes without “affirmative express consent by the owner or lessee,” which must be obtained by a “clear and conspicuous” consent request that is “made in clear and plain language” and that is not a condition “for the use of any nonmarketing feature, capability, or functionality” of the vehicle.

The FTC is further instructed, in consultation with NHTSA, to issue a proposed rulemaking within 18 months of enactment and a final regulation within another 18 months.

As one of the first small steps in Congress’ attempt to regulate in the area of cybersecurity, the SPY Car Act presents a unique intersection of product safety regulation and cybersecurity. There are aspects of the proposed legislation that appear to present technical hurdles, and some of the language used lacks specificity. Clearly the proposed provisions will spark discussion and comment by auto manufacturers, cybersecurity experts and others. Only time will tell whether the SPY Car Act receives sufficient support in Congress for its enactment, whether in its current form or after further revision. Regardless of whether the SPY Car Act, or similar legislation governing cybersecurity threats posed by other consumer products, is enacted into federal law, the potential risks posed by connected consumer products are rapidly gaining the attention of legislators and the public alike. But until more comprehensive federal cybersecurity legislation is passed, and likely even after such legislation is adopted, the safety of such products can be “regulated” by existing state tort law. Given the increasing awareness of the potential consequences of inadequately protected connected consumer products, in designing and manufacturing connected products for sale to consumers in the U.S., manufacturers must consider whether there are technically feasible and reasonable steps that they can take to protect the safety and security of the users of their products from current and emerging cybersecurity threats.

---


4http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/?mbid=nl_72115