Published on *The National Law Review* https://natlawreview.com

Tesla Brings Driverless Technology—and Cybersecurity Concerns—to the Masses

Article By:

Risk Management Magazine

Last week, Tesla Motors unveiled another first for the auto industry: starting immediately, the company will be delivering upgrades directly to vehicles via the Internet.

“We view it the same away as updating your phone or your laptop,” said CEO Elon Musk, as reported in the Wall Street Journal on March 19.

Remote updates for cars was not the only taste of the future that Tesla announced last week. Talk is buzzing even louder about the new “driverless” capability that Tesla’s cars will get this summer (via wireless download, of course). The New York Times says that once your vehicle gets the upgrade, you will be able to turn on an “autopilot” when on major highways.

Tesla’s move further disrupts the traditional way of business in the automotive industry—the direct-to-consumer updates eliminate yet another reason to buy and service through a dealer. The convenience potential to consumers is obvious, and everyone is excited about driverless technology finally being within reach. What could be the downside?

Enter that fear du jour, cybersecurity. Capitol Hill is considering the unpleasant potential of bad guys being able to hack your car’s sophisticated computer system. Last year, Senator Edward Markey (D-MA) sent a letter to 20 car manufacturers asking them about their vehicles’ reliance on wireless computing technology and, in turn, the vulnerability of their systems. In February, he published the companies’ replies, and they weren’t completely reassuring (the full report is here).

According to Wired, Sen. Markey found that “nearly 100%” of vehicles sold today use wireless connections that could be used to access “sensitive systems or [to] compromise privacy.” Combine these findings with the recent exposé on 60 Minutes—where a DARPA hacker demonstrated the ability to hack into a Toyota Prius and gain control of the vehicle’s braking and acceleration—and you have a pretty good understanding of why Sen. Markey is concerned.

Manufacturers that responded to the Senator’s inquiry gave mostly ambiguous answers about the cybersecurity of their products. Some said they encrypt information such as driving history and physical location, while others admitted that they don’t use encryption. The same is true for third-party testing of vehicle cybersecurity—some do it, but many do not.

Tesla was one of three companies that chose not to respond to Sen. Markey's questions. Do concerned consumers have cause to worry? After all, last year, Chinese hackers publicizedtheir successful hack of a Tesla, although they limited their efforts to unlocking the doors and opening the sunroof.

The company is generally tight-lipped, but Musk has said that he is committed to security. He recently stated at a tech conference that "one of the key areas of focus for the company is…protecting…self-driving software from malicious attacks."

Let's hope so. A breach of self-driving software would, of course, be a much bigger problem than the Chinese hack of the car's more superficial systems. And the non-response to Sen. Markey's investigation would then start to resemble a self-inflicted wound.

This article was written by Brandon Right.

National Law Review, Volume V, Number 88