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

Yesterday’s Car Buff Is Today’s Hacker

Article By:

Connor A. Sabatino

If you need any evidence that modern vehicles are becoming more computer than car, look no further than this month’s over-the-air update from ***Tesla Motors*** pushed out to all of its Model S sedans. Like the latest iOS from *Apple* or a Security Update from Microsoft, a car manufacturer has the ability to remotely and automatically implement major changes to already-sold vehicles. Such updates will become increasingly common over time, but also highlight the role software plays in modern vehicles – software that consumers may also try to modify.

On a related note, Tesla Motors recently filed its 2014 annual report with the SEC. In it, Tesla Motors identified as a risk factor the potential for vehicle owners to customize their vehicles:

Automobile enthusiasts may seek to “hack” our vehicles to modify its performance which could compromise vehicle safety systems. . . . We have not tested, nor do we endorse, such changes or products. . . . Such unauthorized modifications could reduce the safety of our vehicles and any injuries resulting from such modifications could result in adverse publicity which would negatively affect our brand and harm our business, prospects, financial condition and operating results.

Hacking cars is nothing new, with car enthusiasts seeking to squeeze every last bit of power out of their vehicle. More recently, the issue has would up in court in Europe over efforts to obtain information about anti-theft systems used by major manufacturers. Hacking a vehicle’s anti-theft system, or its power, are just the first few obvious places for hacking a vehicle. But as Tesla’s Model S demonstrates, the future hacking possibilities are almost limitless.

As vehicle manufacturers more deeply integrate computer software into vehicles, the importance of addressing these issues grows. Some manufacturers may wish to allow the enthusiastic customer – the ‘tinkerer’ – to make some minor modifications. But what are the limitations? Are some of a vehicle’s more critical computers walled-off from other computer systems in the vehicle? Which are connected to wireless communication systems like cellular chips, and which computer systems require a hardwire connection? What are manufacturers doing to protect the source code of these systems? Each of these are important questions to continue asking throughout vehicle development and testing – and eventually, before rolling out over-the-air software updates. Otherwise, as noted by Tesla Motors, manufacturers face potential adverse publicity thanks to the actions of their own enthusiastic customers.

National Law Review, Volume V, Number 92

Source URL:https://natlawreview.com/article/yesterday-s-car-buff-today-s-hacker