From:	Charlie Miller
To:	2015admat
Subject:	Proposed Class 22–Vehicle software–security and safety research follow-up answers
Date:	Sunday, June 07, 2015 12:45:18 PM

Proposed Class 22

Responding party: Dr. Charlie Miller, security researcher

1) I do not think there should be any mandatory disclosing involved with an exception to the dmca for automotive security research. While on the surface, I can understand the desire to want to make sure to protect drivers, you have to understand that disclosure is a very sensitive issue and needs to be handled with care. By limiting the researcher, either by whom they should disclose to or in what time period, you tie their hands into not being able to make the choice that will benefit people most on a case by case issue. For example, suppose a researcher discovered an issue in a particular vehicle's head unit that can be remotely hacked from the Internet, as I plan to present to the public this August. In many cases, reporting this issue to the automotive manufacturer may be prudent. However, what if really the issue is with the head unit itself which was purchased by the manufacturer from a tier 1 supplier. Perhaps it would be better in this case to report directly to the supplier. What if the supplier also provided this head unit to other manufacturers? Might it be best for the researcher to reach out to a 3rd party, such as CERT to coordinate this disclosure? Maybe the researcher wants to verify her results by discussing first with other researchers. Maybe it makes sense to involve the media to get the word out as quickly as possible if patching needs action taken by individual drivers. By restricting whom the researcher may disclose the issue, you may inadvertently constrain the researcher from taking the most prudent course of action in getting the issue fixed and ultimately hurt the people you are trying to protect with this particular provision.

Even putting a time limit on disclosure may often hurt drivers of vehicles. Manufacturers may use this time to delay and not actually work to fix the problem. Without the researching being able to leverage the ability to publicly disclose, the manufacturer is free to ignore the researcher during the time they are forbidden to disclose. If the time given is a function of the manufacturer as opposed to an absolute date (for example, disclosure can not be made until x% of vehicles are patched), the manufacturer may have an incentive not to patch at all (or to do so very slowly) so as to avoid negative publicity which cannot happen if the researcher cannot disclose. Worse yet, the manufacturer may use the time the researcher cannot disclose to prepare lawsuits to stop the researcher from disclosing at all. Ultimately, the any restrictions you place on disclosure will have an impact, and usually a negative one, on how quickly issues are getting addressed.

2) I'll leave to the lawyers.