NATIONAL AUTOMOBILE DEALERS ASSOCIATION
8400 Westpark Drive • McLean, VA 22102
703.821.7040 • 703.821.7041

Legal & Regulatory Group

May 15, 2015

Ms. Jacqueline Charlesworth
General Counsel and Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Avenue, SE
Washington, DC 20559-6001

Re: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07.

Proposed Class 21: Vehicle Software — Diagnosis, Repair, or Modification.

The National Automobile Dealers Association ("NADA") submits the following to the United States Copyright Office regarding its consideration of Proposed Class 21: Vehicle Software — Diagnosis, Repair, or Modification.

This proposed class would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicles, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement.

In reply comments filed on May 1, proponents of this new regulation contend that the law "does not permit the Librarian" of Congress, or the Copyright Office, which advises him in this proceeding, to base its decision on "harms unrelated to copyright infringement." We disagree. The law specifically allows the Librarian to consider "such other factors as the Librarian considers appropriate." 17 USC 1201(a)(1)(C)(v). Respectfully, we submit that it is more than "appropriate" to consider whether heightened risks to vehicle and driver safety and consumer and business data security will be an unintended consequence of the proposed regulation, and, if so, to reject it.

NADA represents over 16,000 franchised automobile and truck dealers who sell new and used motor vehicles, and engage in service, repair, and parts sales. Together our members employ in excess of one million people nationwide. NADA is particularly focused on the integrity and security of the automobile data ecosystem and that of the American automotive infrastructure. We submit these comments because we are concerned about the potential risks to dealers and the

driving public that could result from allowing access to computerized control systems for automobiles.

There are a number of concerns that dealers have about Proposed Class 21. Foremost among these are the safety and security implications. Today's automobiles are not only vastly different than smart phones, appliances, video games or other computerized consumer goods, they are vastly different than the automobiles of just a few years ago. Allowing consumer access to vital computerized systems within an automobile has several potential negative effects. First, because of the interconnected nature of the vehicle systems and the ever-increasing number of "driver-assist" or "self-driving" features appearing in automobiles, access to seemingly innocuous systems (such as emissions) could inadvertently cause failure in critical systems (such as braking or steering).

Second, given the increasingly interconnected nature of automobiles[1] with each other and with the transportation infrastructure, access to one vehicle not only jeopardizes the safety and security of that driver and any members of the driving public that vehicle interacts with, it is ultimately could endanger us all. The safety implications of a virus or malware that has been introduced (intentionally or otherwise) into an automobile that could be transmitted to other vehicles or the infrastructure is potentially catastrophic. Simply put, it is no longer a question of whether consumers should be allowed to "tinker" with their own vehicle it is whether they should be able to tinker with the transportation infrastructure.

Dealers are at the front line of these issues and see the harm that such access can cause. When consumers cause damage to their vehicles through attempted vehicle modification via computerized systems, that vehicle is often brought to the dealership for repair. It can be difficult for a dealer to determine the cause of the failure, and consumers are often unaware that such modification efforts can void or limit their manufacturer warranty. In some cases, unfortunately, some consumers may even fail to disclose their tampering in order to obtain a repair covered by the warranty. Whether intentional or inadvertent, this can lead to customer disputes and unhappiness that dealers must often mediate.

Dealers are particularly concerned with the potential safety risks to *dealership employees* who are working on a vehicle with undisclosed software modifications. Because these systems control vital vehicle functions, there are numerous ways that dealership employees could be physically injured or endangered – dangers that do not exists with physical modifications -- if such software modifications were permitted.

In addition, dealers are increasingly concerned with the potential effect on dealer systems that may result from such consumer access. Imagine a vehicle that has been infected with a virus or other malware due to a consumer's software modification efforts, that is then brought into the dealership service department for repair. Such infected systems pose a very real risk of infecting not only dealer systems (which contain tremendous amounts of sensitive consumer data), but also other vehicles that members of the public bring in for repair and are thereby connected to those same dealer systems.

---

[1] *See, e.g.*, http://www.nhtsa.gov/About+NHTSA/Press+Releases/2015/nhtsa-will-accelerate-v2v-efforts; http://www.dot.gov/BeyondTraffic ; http://www.dot.gov/sites/dot.gov/files/docs/TheBluePaper.pdf; http://www.safercar.gov/v2v/index.html.

Cars are also unlike other devices or appliances in that they generally have multiple owners. We urge you to consider the uncertainty, concern, and potential danger that will be created by introducing automobiles that have undisclosed software modifications into the used car stream of commerce. Even if the first (or current) owner of a vehicle feels they have a "right" to modify the software on that vehicle, we believe that subsequent owners have strong competing interests as well. Of course automobile dealers are the largest purchasers of used vehicles in the marketplace, and we believe that such unfettered modification to vehicle computer systems could create havoc in the used car market, with the bulk of the harm falling on unsuspecting consumers who either purchase such vehicles, or who after purchase find that their vehicle is worth substantially less due to such tampering.

Of course the overwhelming majority of vehicle owners do not wish to tamper with the safety, emissions, or other computerized functionality of their vehicle. Far from it, most drivers are supremely concerned with vehicle safety and look to the manufacturers and their franchised dealers to ensure that vehicles are operating in a safe and compliant manner. While dealers certainly understand the frustration that certain individuals who wish to modify their car may feel at restrictions on access to certain vehicle systems, we believe that allowing such access causes unnecessary and potentially profound safety, environmental, and other risks that far outweigh any potential inconvenience.

There are a number of other reasons that, in our view, such an exemption is inappropriate and counterproductive. One of which is the need to tread *very* carefully in this area and to defer fully to the safety of the driving public - especially at this point in time where such profound changes are being made to the way we drive. There will be tremendous debate about balancing interests in designing the transportation system of the future. However, we believe that security and integrity must be a nonnegotiable fundamental in these systems if these changes are going to bring the massive efficiencies and safety gains envisioned.

We would be very happy to provide further details at any time. Please do not hesitate to contact us if we can help in any way with your efforts going forward.

Thank you for your consideration of our remarks.

Sincerely,

/s/

Bradley T. Miller

Director, Legal and Regulatory Affairs