

Before the
U.S. Copyright Office
Library of Congress
Washington, DC

In the Matter of

Exemption to Prohibition on)
Circumvention of Copyright) **Docket No. 2014-07**
Protection Systems for Access)
Control Technologies)

**Short Comment Regarding a Proposed Exemption
Under 17 U.S.C. 1201**

Item 1. Commenter Information

This comment is submitted on behalf of the SAE Vehicle Electrical System Security (VESS) Committee, and any questions can be addressed to:

William Gouse, Director, Federal Program Development, SAE International, 202-434-8944, wgouse@sae.org

Item 2. Proposed Class Addressed

Proposed Class 17 – Jailbreaking – all-purpose mobile computing devices

This class of exemption seeks to remove TPMs and/or allow circumvention of existing TPM for devices that fit the category of “all-purpose mobile computing devices”. EFF, et al., seek to extend such an exemption granted for mobile handset devices by The Librarian during the prior two triennial proceedings, to tablets and other devices which fit the description of an ‘all-purpose mobile computing’ device.

Item 3. Statement Regarding Proposed Exemption

As publicly discussed during several SAE VESS Committee meetings, we recommend that The Librarian keep the following seven technical points in mind while considering an exemption under the Proposed Class 17 for ‘jailbreaking’:

1. The VESS Committee’s scope pertains to on-board vehicle electrical systems that affect vehicle control or otherwise acts contrary to a vehicle occupant’s interests if the systems are manipulated by an attacker. The committee’s goals are (i) identify and recommend strategies and techniques related to preventing and detecting adversarial breaches, and (ii) mitigating undesirable effects if a breach is achieved. The committee is currently working to classify attack methods, propose preventative strategies, define levels of security by criticality of system type, and identify architecture-level strategies for mitigating attacks.
2. It is our consensus that on-board vehicle electrical and electronic systems which affect vehicle control and ensure safe operation of a vehicle might fall under the description of the category of ‘all-purpose mobile computing devices.’ This is due to the fact that increasingly, vehicle software uses similar operating systems (e.g., Linux, Android, Windows) to those of underlying mobile phones and tablets, in order to support the large demand from consumers for in-vehicle entertainment and productivity applications requiring connectivity (e.g., WiFi, Bluetooth, 4G LTE, etc.). Besides the operating system, the underlying hardware being used

in vehicle electrical and electronic systems (general purpose, multi-media capable processors, etc.) also might fall under the description of ‘all-purpose mobile computing.’

3. However, vehicle-embedded computing systems should not be viewed in the same light as other systems for which previous exemptions have been granted. This is due to the fact that a significant portion of the code is needed to comply with existing safety & emission regulations, and is capable of affecting the operation of the vehicle. Vehicle systems are by nature cyber-physical. Any TPM circumvention techniques developed for the purposes stated in the proposed exemptions, also have a significant potential for abuse, at a large scale by malicious entities, leading to a threat to public safety and critical infrastructure.
4. The automotive vehicle is not an all-purpose mobile computing device, and a distinction needs to be made here. It does comprise computing devices, computerized and connected modules, communication networks, but it has a strong physical/mechanical/kinetic component that sets them apart from general purpose mobile devices. The term ‘cyber-physical’ system is hence used for automotive vehicles as opposed to a general purpose mobile computing device. We have a genuine concern about people getting access to the systems within the automotive vehicle. If changes are made to these systems, without following due process of testing and validation, then there is very likely to be harmful side effects emerging on subsequent operation. With such a powerful kinetic component to the operation of these vehicles, serious harm can be caused to drivers, passengers, pedestrians, and occupants of other vehicles.
5. For example, as the industry incorporates new technologies including more ‘by-wire’ features, tampering with these systems can result in making them inoperable or unsafe. This could result in serious harm, if for example the brakes became inoperable. Similarly, one can imagine the detrimental effect of disturbing the calibration or otherwise affecting the operation of blind spot warning systems, or forward collision warning systems, potentially leading to improper operation which might cause a vehicle to stop abruptly.
6. It may be worthwhile for The Librarian to keep in mind the fundamental difference between vehicle control systems, and mobile phones & tablets. We do not recommend combining both under the same category of ‘all-purpose mobile computing devices’ due to the nature of the systems and the existing vehicle regulatory requirements.
7. It is our recommendation that if The Librarian were to consider an exemption under this class 17, ‘all-purpose mobile computing devices,’ then vehicle-embedded computing devices should be excluded from the list of devices for which this exemption applies.

The SAE VESS Committee stands ready to assist the Copyright Office in providing and sharing its technical expertise with respect to any future issue discussed within Proposed Class 17.