MITCHELL SILBERBERG & KNUPP LLP
A LAW PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

MS&K

Steven J. Metalitz
A Professional Corporation
(202) 355-7902 Phone
(202) 355-7892 Fax
met@msk.com

June 29, 2015

VIA E-MAIL ONLY (2015ADMAT@LOC.GOV)

Jacqueline C. Charlesworth
General Counsel and Associate Register of
Copyrights
U.S. Copyright Office
Library of Congress
101 Independence Ave SE
Washington, DC 20559-6000

Re: Docket No. 2014-7, Exemptions to Prohibition Against Circumvention of Technological Protection Measures Protecting Copyrighted Works, Class 22

Dear Ms. Charlesworth:

On behalf of the Alliance of Automobile Manufacturers ("Auto Alliance"), attached please find the response of the Auto Alliance to your letter of June 3, 2015 regarding Proposed Class 22 – Vehicle Software – security and safety research.

Thank you for this opportunity to respond to these questions, and please let me know if we can provide any further information.

Sincerely,

Steven J. Metalitz

MITCHELL SILBERBERG & KNUPP LLP

ATCH AS STATED

1818 N Street, NW, 8th Floor, Washington, DC 20036-2406
Phone: (202) 355-7900 Fax: (202) 355-7899 Website: WWW.MSK.COM

Post-Hearing Questions, Class #22

Responses of Alliance of Automobile Manufacturers (Auto Alliance)

1. *Given concerns raised by participants regarding disclosure of research results to manufacturers, please provide any additional thoughts you may have as to how the Office might approach this issue if it were to recommend the requested exemption. If some sort of disclosure to the manufacturer were required, what would that process be? Please address any relevant First Amendment or regulatory issues in your response.*

For the reasons stated in our previous submissions and testimony, Auto Alliance does not believe that the record in this proceeding would support the recognition of any proposed exemption regarding security research applicable to the automobile sector. Proponents have failed to demonstrate any adverse impact on legitimate security research activities that is attributable to 17 USC § 1201(a)(1), and/or that would be substantially ameliorated by granting an administrative exemption making that provision inapplicable to circumvention for the purpose of such research. The May 19 hearing testimony further reinforced this pattern of proponents' complete failure to carry their burden on this critical issue. [1] Indeed, in detailing his current security research at the hearing, independent researcher Charlie Miller, who testified that he has kept one manufacturer regularly updated as to the findings of his research project on that company's vehicles, stated that the manufacturer's response has not been to threaten litigation but instead to say "thank you. "[2]

As noted in our previous submissions and testimony, automobile manufacturers increasingly collaborate with independent researchers in a number of fora to advance the industry's paramount goal of improving safety and security for drivers, passengers, and members of the public. When auto manufacturers enter into contractual arrangements with capable researchers, these arrangements generally address the terms and conditions under which findings will be disclosed to the manufacturer, and to the general public. Under these terms and conditions, if the research identifies any significant safety or security vulnerabilities, these will be fully and promptly disclosed to the manufacturers, who will have enough time to design and implement any needed corrections. Any disclosure to the general public would be timed and managed to minimize the risk that the information disclosed would enable bad actors to exploit the vulnerabilities identified. We believe that these negotiated arrangements present the optimal model for resolving the issue of disclosure to the manufacturer and to the general public. However, if a security research exemption applicable to automobiles were granted, these negotiated arrangements would not apply to researchers who chose simply to rely upon the exemption, rather than to enter into collaborative projects with manufacturers. Some researchers might choose to follow Mr. Miller's example of prior disclosure to the manufacturer, so that the latter has ample time to fix any issues before publication[3]; but others surely will not.

An approach that the Office should consider, if it determines that it will recommend an exemption in this area but wishes to encourage disclosure in a responsible manner, would build

[1] *See, e.g.*, Class 22 Hearing Transcript, at 37 (May 19, 2015) *and* Class 22 Hearing Transcript, p. 42-43 (May 19, 2015) (Mr. Miller is unable to give any concrete examples of research not undertaken or published specifically due to fear of litigation under the DMCA).
[2] *Id*. at 47.
[3] Class 22 Hearing Transcript, at 46 (May 19, 2015).

into the administrative exemption some of the safeguards that Congress thought to be important when it enacted the closely related statutory exception for security testing (17 USC § 1201(j)). This is the approach that the Librarian (on the Office's recommendation) followed in 2010, the last time he recognized an exemption in this proceeding for security testing.[4] In that cycle, the Register concluded that "the Section 1201(j) exemption demonstrates Congress's judgment as to the conditions under which circumvention for the purpose of security testing should be permitted;" she was "persuaded that the means of tailoring the class of works [for an administrative exemption] should be guided by Congress's general approach to the problem in Section 1201(j)"; and she recommended that the exemption should be subject to "conditions … which are modeled on the conditions Congress included in Section 1201(j)" in order to "remain faithful to Congress's judgment."[5]

Building on this template, if the Office decides to recognize a security research exemption applicable to automobiles, it should consider (1) restricting any exemption to acts carried out solely for the purpose of "good faith security research";[6] (2) making the exemption inapplicable unless the information derived from the research is shared directly with the manufacturer, in a manner that enables the manufacturer to respond effectively to any security or safety vulnerabilities identified;[7] and (3) conditioning the exemption on such information being used or maintained only in a manner that does not facilitate infringement under Title 17 or a violation of applicable law other than section 1201(a)(1)(A), including a violation of privacy or breach of security.[8] This approach would have the merit of "remaining faithful to Congress's judgment" that any exceptions in this area should be approached with prudence and caution towards the disclosure of results, with a strong bias in favor of requiring prior disclosure.

While an exemption embodying these conditions would inevitably be less specific than one which defined a set prior disclosure period and the manner in which the disclosure must be made to trigger the running of that period, it would at the same time avoid a number of serious difficulties with the latter approach. To mention only two:

---

[4] Although, as noted in our submissions, the 2010 security testing exemption was based on a factual record completely unlike the one compiled in this proceeding, and therefore provides no precedent for recognizing any security research exemption in this proceeding, the approach taken by the Office in fashioning the terms of the exemption recognized in 2010 is highly relevant if the Office decides to recommend doing so in this cycle.

[5] Recommendation of the Register of Copyrights in RM 2008-8; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 201, 203, n. 666 (June 11, 2010) ("2010 Recommendation").

[6] *Cf.* 17 USC § 1201(j)(1) (incorporating "good faith" requirement in definition of "security testing") *and* 2010 Recommendation 4 (exemption limited to circumvention "solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities").

[7] *Cf.* 17 USC 1201(j)(3)(A) ("whether the information derived from the security testing was …. shared directly with the developer of such computer, computer system or computer network") *and* 2010 Recommendation 4(i) (exemption applies only if "the information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network," mirroring a parallel provision of section 1201(j)(3)(A).

[8] *Cf.* 17 USC 1201(j)(3)(B) ("whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security") *and* 2010 Recommendation 4(ii) (exemption applies only if "the information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law").

- There is no single definable time frame within which customers would no longer be at risk from public disclosure of a vulnerability identified through use of the exemption. Cars are operated by customers, with whom manufacturers have no direct contractual relationship (all auto sales are through dealers or other third or fourth parties), and whose actions the manufacturers cannot control. Manufacturers rely upon customer participation in field actions to fix defects, including vulnerabilities. An effective software fix to address any identified vulnerability will take time to develop and test, and likely even more time to implement, as owners of vehicles subject to the vulnerability would need to be located and notified; patches would need to be distributed to dealers and independent repair facilities, who would require training on their installation; and vehicle owners would need time to bring their vehicles to the repair facilities for testing and (where needed) installation of the patch. If addressing the vulnerability in question required a change in vehicle hardware, the implementation path could be even longer, if a new or modified part needed to be designed, tested, and put into mass production. Given these facts, it is not possible to determine in advance a time period after which public disclosure of the vulnerability would be safe. Precedents from other industries (for example, consumer software markets) in which the circumstances are different would be of no value in determining the appropriate prior disclosure time frame for the auto industry. The auto industry today generally lacks the ability to provide software fixes via download to registered end-users, and it cannot assume that its customers have the connectivity, the equipment, and/or the technical expertise to install a patch on their own.

- Such a prescriptive disclosure requirement would raise significant First Amendment issues. Forcing independent researchers to report to manufacturers is a form of compelled speech, while restrictions placed on researchers' use and disclosure of their research results raise other First Amendment concerns. In both cases, the permissible extent of those limits may be highly fact dependent, including issues both of the content of the disclosure and the manner in which it is made. The challenge of embodying these specific restrictions in a DMCA exemption promulgated by the Librarian is thus likely to be insurmountable, both upon practical and constitutional grounds.

2. *Please briefly address how the proposed exemption might relate to or be limited by other federal or state laws or regulations, including but not limited to the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, and any other statutory or regulatory provisions.*

As noted above, if any exemption is recognized for security research on automobiles, it should follow the pattern set by Congress in enacting section 1201(j) and by the Librarian in fashioning a security testing exemption in 2010. The exemption should not apply in any case in which security research activities constitute a violation of any other applicable law, including specifically 18 USC § 1030, and other provisions of the Computer Fraud and Abuse Act; and it should not apply if the security research results are used or maintained in a manner that facilitates copyright infringement or any other violation of applicable law.