

June 29, 2015

VIA ELECTRONIC MAIL

Jacqueline C. Charlesworth
General Counsel and Associate Register of Copyrights
United States Copyright Office, Library of Congress
101 Independence Avenue SE
Washington, DC 20559-6000
2015admat@loc.gov

RE: Proposed Class 25 - Security research

Docket 2014-7 Exemptions to Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works

Dear Ms. Charlesworth:

General Motors, LLC (“GM”) respectfully submits the following response to the questions set forth in the U.S. Copyright Office’s June 3, 2015 letter related to Proposed Class 25 - security research.

- 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.**

As set forth in GM’s comments submitted on March 27, 2015 (“Comments”), GM opposes any exemption that would allow the public disclosure of security and safety vulnerabilities, even if such exemption were to require disclosure to manufacturers, because the public disclosure of such vulnerabilities in vehicle software still creates significant safety and security risks as set forth below.

New vehicles are already twice removed from the manufacturer by the time they reach their initial owners, and even further removed for used cars. Cars are sold from manufacturers to dealers and then on to end users. Therefore, when manufacturers identify vulnerabilities and create software patches, they require the cooperation of vehicle owners, often times owners with whom the manufacturer and the dealer have no relationship, to implement the fix. Manufacturers can issue recalls and service bulletins to inform vehicle owners of a software patch, but cannot issue over the air software patches without vehicle connectivity, which a consumer may not subscribe to or could cancel at any time. Accordingly, there are a significant number of vehicles that lack the ability to receive an over the air software patch. Thus, there are numerous

challenges to fixing a security and safety vulnerability for a product like a car which are exacerbated by the fact that there are over 250 million cars on the road in the United States today.

Such challenges are highlighted when considering statistics associated with more traditional vehicle recalls. The government estimates that thirty percent of cars do not get fixed when recalls are issued, which is more than one out of every five cars in the U.S. See www.carfax.com/blog/airbag-recalls-nationwide. Moreover, the failure to repair vehicles that have been recalled is more likely when subsequent vehicle owners are not aware they have purchased a vehicle subject to an open recall.

Manufacturers' reliance on vehicle owners to bring in their cars to fix a recall and the reality that many owners do not fix identified vulnerabilities means that even a prior disclosure scheme which allows for later publication of vehicle software vulnerabilities could leave millions of driver at risk, particularly where history and reality dictate that many vehicle owners do not participate in the fixes auto manufacturers already offer when recalls issue.

Accordingly, even prior or contemporaneous disclosure would create safety and security risks if software vulnerabilities are publically disseminated and the only way to ensure vehicle safety and security is for such research to be conducted in cooperation with the manufacturer as set forth in GM's Comments. Furthermore, as intimated by Dr. Green in his comments submitted on May 1, 2015 ("Green Comments") and in the testimony of Blake Reid during the May 26, 2015 rulemaking hearings, any disclosure standard could raise First Amendment issues. See Green Comments, p. 15 see also Testimony of Blake Reid, Sixth Triennial 1201 Rulemaking Hearings Transcript (May 26, 2015) at 85:8 -85:18 (stating that ". . . it's important to underscore that, when we're talking about the disclosure of research, we're talking about First Amendment-protected speech. So you've got some serious limitations on the level of prior restraint that you can apply. . . ."). The Security Researchers also indicate that the protection afforded by the First Amendment to security vulnerability disclosures is limited. See the comments of the Security Researchers submitted on May 1, 2015, p. 5, p.5, FN 11 (citing an article, see pg. 1, stating that "the Supreme Court has never articulated the extent of First Amendment protection for . . . factual speech that may be repurposed for crime.").

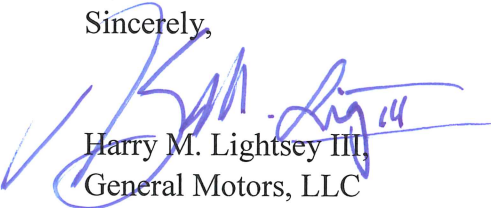
2. Please briefly address how the proposed exemption might relate to or be limited by other federal or state laws or regulations, including but not limited to the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, and any other statutory or regulatory provisions.

The proposed exemption would allow security researchers to publish information that could then be used to violate various laws. Indeed, as noted in GM's Comments, allowing the exemption is akin to authorizing publication of an instruction manual for circumvention of safety and regulatory protocols in a vehicle and a roadmap to accessing highly sensitive and carefully calibrated vehicle software to which access is in part limited for security reasons. For example, circumvention of

certain emissions-oriented TPMs, such as seed/key access control mechanisms, could be a violation of various federal laws. Notably, the Clean Air Act (“CAA”) prohibits “tampering” with vehicles or vehicle engines once they have been certified in a certain configuration by the Environmental Protection Agency (“EPA”) for introduction into U.S. commerce. “Tampering” includes “rendering inoperative” integrated design elements to modify vehicle and/or engine performance without complying with emissions regulations. In addition, the Motor Vehicle Safety Act (“MVSA”) prohibits the introduction into U.S. commerce of vehicles that do not comply with the Federal Motor Vehicle Safety Standards, and prohibits manufacturers, dealers, distributors, or motor vehicle repair businesses from knowingly making inoperative any part of a device or element of design installed on or in a motor vehicle in compliance with an applicable motor vehicle standard. The disclosure of information relating to the ECUs controlling functions relating to fuel consumption and emissions threatens to undermine this regulatory landscape. Further, third parties can rely on published information to defraud computer owners in violation of 18 U.S.C. 1030, which, *inter alia*, makes it illegal for an individual to knowingly and with intent to defraud, access a protected computer without authorization and by means of such conduct further the intended fraud and obtain anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

We hope the foregoing has been helpful to the Office in its rulemaking proceeding. If you have any further questions, please do not hesitate to contact us.

Sincerely,



Harry M. Lightsey III,
General Motors, LLC