*Before the*

**U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS**

**In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201**

**Docket No. 2014-07**

**Response of Electronic Frontier Foundation to June 3, 2015 Copyright Office Questions on Proposed Class 22**

## 1. Commenter Information:


Kit Walsh
Corynne McSherry
Mitch Stoltz
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
rulemaking-2015@eff.org

*Counsel for EFF:*
Marcia Hofmann
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664


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.**

A Disclosure Restriction Would Be Unnecessary and Counterproductive

At the May 19, 2015, hearing, the representatives of the Copyright Office asked for comment regarding a hypothetical requirement that disclosure to a manufacturer take place some period of time before disclosure to anyone else, in order for a researcher to be covered by an exemption.

Such a limitation is not necessary or wise for the reasons briefed and discussed at the hearing. The record shows auto manufacturers have ignored important security findings, meaning that restricting researchers' ability to disclose to others simply makes drivers less secure.

If the Office considers limitations related to disclosure, it should keep in mind the cases where:

- Drivers who were informed of the vulnerability could take steps to protect themselves;
- Third parties may be faster to fix vulnerabilities than the manufacturer, which has an interest in not admitting fault;
- Multiple researchers collaborate and communicate amongst themselves or as part of a community (possibly online);
- Multiple manufacturers suffer from the same or related vulnerabilities, either independently or due to reliance on a common vendor;

- A security researcher evaluates a system, finds no vulnerability, and wishes to say so;
- An individual unintentionally finds a vulnerability in the course of some other activity; or
- A manufacturer has a track record of ignoring security-related disclosures or of hostility to independent research.

Furthermore, no party has provided an argument against the prompt disclosure of *safety* research (such as scrutinizing vehicle code to detect bugs that might lead to unintended acceleration or lead to failure of airbag deployment).[1] The (misguided) rationale against disclosure of *security* research is based on hypothetical bad actors learning how to hack a vehicle and the theory that this outweighs the benefits of prompt and widespread disclosure, but this rationale cannot apply to safety issues. Where the danger arises not from a hypothetical attacker, but from the operation of the software itself, it is all the more clear that the public should be made aware so they can avoid dangerous conditions and vehicles.

Disclosure Restrictions Would Be Unconstitutional Prior Restraints on Speech

Just as the First Amendment prohibits the norms of responsible conduct in the press from being written into law, the same is true for disclosures of software flaws. *See Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 560 (1976); *Ostergen v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010) (disclosure of social security numbers to demonstrate scope of government computer vulnerability was protected speech).

Dictating which research disclosures are lawful and which result in liability would create an unconstitutional prior restraint on speech. A prior restraint on speech must satisfy exacting First Amendment scrutiny, which it can rarely do. *Organization for a Better Austin v. Keef*e, 402 U.S. 415, 419 (1971); *New York Times Co. v. United States,* 403 U.S. 713, 714 (1971). A system of prior restraint can be justified only in extremely narrow circumstances and the censorship regime must include procedural safeguards to ensure a judicial, case-by-case review of the censor's decisions. *See id.; Freedman v. State of Md.*, 380 U.S. 51, 58-59 (1965) (describing procedural requirements, including concrete standards, judicial review and appeal, and the requirement that the burden of proof lie with the censor).

This is also true of regulations that delay, rather than outright prohibit, protected speech. *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 560-61 (1976). In *Nebraska Press*, the Supreme Court was faced with a temporary order banning reporting on certain subjects to protect a defendant's right to a fair trial, and commanding reporters to adhere to a previously-voluntary set of professional norms. *Id.* at 543. The order lasted only until a jury was impaneled. *Id.* It was an improper prior restraint on speech because timeliness is important to the function of reporting on newsworthy events and because the giving legal effect to norms around news reporting is contrary to the freedom guaranteed by the First Amendment. *Id.* at 560-61.

When some might abuse their freedom of speech – something that has not been demonstrated here – this cannot justify repressing such freedoms for others:

[1] EFF discussed this issue in its reply comments of May 1, 2015.

> *[A] free society prefers to punish the few who abuse rights of speech after they break the law than to throttle them and all others beforehand. It is always difficult to know in advance what an individual will say, and the line between legitimate and illegitimate speech is often so finely drawn that the risks of freewheeling censorship are formidable.*

*Se. Promotions, Ltd. v. Conrad*, 420 U.S. 546, 559 (1975).

Even those restrictions that do not constitute prior restraints, but are based on the content of speech or the identity of the speaker or audience, are subject to strict scrutiny and must be narrowly tailored to achieve a compelling government interest. *Police Dep't of City of Chicago v. Mosley*, 408 U.S. 92, 95 (1972); U.S. West v. FCC, 182 F.3d 1224, 1232 (10th Cir. 1999) ("Effective speech has two components: a speaker and an audience. A restriction on either of these components is a restriction on speech. ").

Setting aside the overbreadth of a categorical prohibition on speech, the Supreme Court has explained that even *particular* speech that goes so far as to *advocate* lawbreaking cannot be punished consistent with the First Amendment unless it meets the *Brandenburg* test for speech that is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969). The First Amendment goes so far as to protect advice to gang members on what kind of criminal activities might improve their gang's standing. *McCoy v. Stewart*, 282 F.3d 626, 632 (9th Cir. 2002) (granting habeas petition because of "definite and firm conviction" that Arizona courts erred in allowing the punishment of defendant's speech).

A disclosure restriction in the exempted class would be a restriction based on content and audience, requiring strict scrutiny. It would fail, because it would not be a narrowly tailored means to address any compelling government interest. A requirement dictating disclosure practices would inevitably forbid disclosures having no connection to any crime or tortious conduct. It would also be counter-productive, preventing researchers from exerting the watchdog pressure needed to ensure flaws are fixed in a timely fashion. The government interests in preventing malicious hacking are served by laws against such hacking; restricting publication of software flaws would be an overly-broad attempt at a remedy.

A researcher may not be penalized for disclosing truthful information about flaws in vehicle software.[2] The Supreme Court in *Brandenburg* considered Ku Klux Klan rallies and propaganda advocating violence against minorities. 395 U.S. at 445-46. The research disclosures at issue here do not come close to the danger level of the speech that was *protected* in that case. Researchers here are sharing information, typically in a responsible way, and none of them are advocating unlawful conduct. Certainly none are intentionally inciting others to break the law imminently, or indeed in any way. The First Amendment clearly will not permit punishment of research disclosures based on speculation about future lawless acts of vehicle hacking.

[2] Unless the disclosure violates a preexisting duty to keep the information confidential, involves disclosure of purely private information, or somehow can be punished as falling within an unprotected category of speech. None of these scenarios apply here, and no one has argued that they do.

It would be antithetical to the purpose of copyright law and the command of the First Amendment to constrain the dissemination of true, newsworthy information about software flaws. This rulemaking is a safety valve in Section 1201 that is necessary to *protect* First Amendment values, including fair use and the idea/expression dichotomy.[3] Accordingly, the proposed exemption should be granted without assigning force of law to any particular norms of disclosure and without punishing speech merely because a malicious actor might learn something from it.

**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.**

There are several areas of law that affect computer system research generally. The DMCA is unique in that it makes it possible for a device owner to be liable for research done entirely on their own hardware or with the permission of the hardware owner. The proposed exemption relates to this narrow range of research activities, being limited by its own terms to research done by or on behalf of the vehicle owner. It does not (and cannot) have any effect on the scope of other laws, such as the CFAA.

Nor does the CFAA apply to the conduct of a researcher circumventing access controls on a device they own, or at the behest of the device owner. The CFAA hinges on whether the person accessing a protected computer does so without or beyond the authorization of the owner of the protected computer. Even the most expansive interpretations of the CFAA do not reach the conduct of a computer owner accessing information on their own device. *See United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (CFAA liability depends on relationship "between the computer owner and the user."); Department of Justice Office of Legal Education, *Prosecuting Computer Crimes* (2015), available at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (articulating prosecutors' broad view of CFAA), Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003) (describing broad interpretations of CFAA).

In the event that there were some edge case in which conduct within the exempted class somehow violated the CFAA, the grant of the exemption would have no impact on CFAA liability. In other words, such conduct would remain prohibited by the CFAA even if an exemption were granted that eliminated DMCA liability for the conduct. The same is true for other areas of law, such as wiretap laws, vehicle-specific regulations, and tort law.

The Copyright Office does not need to evaluate the entire universe of laws that might apply to vehicle software researchers. EFF explained in its June 2, 2015, comments that Congress narrowed the inquiry from whether the adversely affected uses were "lawful" to whether they are "noninfringing." And even the original draft language specified lawfulness "under title 17," so

[3] Even if one viewed this rulemaking a conferring a "benefit" rather than vindicating rights to use copyrighted works, conditions on a benefit that implicate speech (such as disclosure requirements) would have to satisfy First Amendment scrutiny just as pure restrictions would. *See Bd. of County Commissioners v. Wabanusee County*, 518 U.S. 668, 674 (1996); *Bullfrog Films v. Wick*, 847 F.2d 502 (9th Cir. 1988).

that it also could have been read to restrict the inquiry to copyright-related concerns. The Copyright Office has recognized the "narrower focus" of the language in the enacted version of Section 1201.[4] It should not now discard the guidance Congress provided in Section 1201 regarding the scope of the rulemaking. Other laws are not impacted by this rulemaking, and neither is this rulemaking impacted by those other laws.

[4] Marybeth Peters, *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*, The Register of Copyrights, at 6 n.9 (June 11, 2010), available at http://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf.