

## Petition to Renew a Current Exemption Under 17 U.S.C. § 1201

Please submit a separate petition for each current exemption for which renewal is sought.

**note:** Use this form if you want to renew a current exemption without modification. If you are seeking to engage in activities not currently permitted by an existing exemption, including those that would require the expansion of a current exemption, you must submit a petition for a new exemption using the form available at <https://www.copyright.gov/1201/2018/new-petition.pdf>.

If you are seeking to expand a current exemption, we recommend that you submit both a petition to renew the current exemption without modification using this form, and, separately, a petition for a new exemption that identifies the current exemption, and addresses only those issues relevant to the proposed expansion of that exemption.

### Item A. Petitioners and Contact Information

Please identify the petitioners and provide a means to contact the petitioners and/or their representatives, if any. The “petitioner” is the individual or entity seeking renewal.

Andrea Matwyshyn, Professor of Law/ Professor of Computer Science (by courtesy), Northeastern University/  
Visiting Research Collaborator, Center for Information Technology Policy, Princeton University/ Affiliate  
Scholar, Center for Internet and Society, Stanford Law School

On behalf of

“The Security Researchers”

Steven Bellovin, Professor of Computer Science, Columbia University

Matt Blaze, Associate Professor, Computer and Information Science, University of Pennsylvania

Nadia Heninger, Magerman Term Assistant Professor, Computer and Information Science, University of Pennsylvania

**Privacy Act Advisory Statement:** Required by the Privacy Act of 1974 (P.L. 93-579)

The authority for requesting this information is 17 U.S.C. §§ 1201(a)(1) and 705. Furnishing the requested information is voluntary. The principal use of the requested information is publication on the Copyright Office website and use by Copyright Office staff for purposes of the rulemaking proceeding conducted pursuant to 17 U.S.C. § 1201(a)(1). NOTE: No other advisory statement will be given in connection with this application. Please keep this statement and refer to it if we communicate with you regarding this petition.

U.S. Copyright Office · Library of Congress · 101 Independence Avenue SE · Washington, DC 20557-6400 · [www.copyright.gov](http://www.copyright.gov)

PETITION TO RENEW A CURRENT EXEMPTION UNDER 17 U.S.C. § 1201 REV: 06 / 2017

## Item B. Identify Which Current Exemption Petitioners Seek to Renew

Check the appropriate box below that corresponds with the current temporary exemption (see **37 C.F.R. § 201.40**) the petitioners seek to renew. Please check only one box. If renewal of more than one exemption is sought, a separate petition must be submitted for each one.

- Computer programs that operate devices and machines primarily designed for use by individual consumers (including voting machines), motorized land vehicles, or medical devices designed for implantation in patients and corresponding personal monitoring systems, for purposes of good-faith security research**

## Item C. Explanation of Need For Renewal

Provide a brief explanation summarizing the continuing need and justification for renewing the exemption. The Office anticipates that petitioners may provide a paragraph or two detailing this information, but there is no page limit. While it is permissible to attach supporting documentary evidence as exhibits to this petition, it is not necessary. Below is a hypothetical example of the kind of explanation that the Office would regard as sufficient to support renewal of the unlocking exemption. The Office notes, however, that explanations can take many forms and may differ significantly based on the individual making the declaration and the exemption as issue.

We are computer science academics who research computer security for purposes of improving the security and reliability of systems used by the public. We were the proponents of the good-faith computer security research exemption granted during the last 1201 rulemaking process. As we explained in our original petition and responses during that process, the research we conduct directly impacts both national security and consumer protection as well as copyright interests.

Through our work, we have personal knowledge that the granted exemption has materially improved the ability of security researchers such as ourselves to conduct, publish, and publicly present the results of security research. We also have personal knowledge that the need for the exemption continues to exist, and we have no reason to believe that this need will abate during the next triennial period. We have personally been involved with security research that has relied on the exemption, and we regularly engage with other security researchers who have similarly informed us that their research and creation of follow-on creative works has relied on and been enabled by the existence of this exemption. For example, in July 2017, the DEF CON computer security conference purchased a series of electronic voting devices and held a workshop on voting security. In reliance on the exemption, several thousand members of the computer security community were able to examine, audit, and test a variety of electronic voting equipment used in U.S. elections. A number of the participants discovered ways to manipulate the security of these voting devices in ways that could impact outcomes of elections. The results of this research will be published and publicly presented, enabling election officials to improve the security of their systems prior to the next election. Additionally, Consumer Reports has newly begun testing the quality of computer code in certain consumer products and disseminating the results of this research to the public. In brief, the existence of the exemption is improving computer security in ways that benefit both consumers and national security while stimulating the creation of new creative works. Without the continued existence of this exemption, this progress would be halted or at least substantially hindered.

As was the case three years ago, consumer-facing products including Internet of Things home devices,<sup>1</sup> cars,<sup>2</sup> and medical devices<sup>3</sup> continue to suffer from security flaws raising consumer protection and national security concerns. Manufactures of these devices do not always identify and correct these code flaws prior to releasing products into the market, and, in some cases, manufacturers continue to be resistant to acknowledging the existence of flaws when security researchers contact them to report findings of security vulnerabilities.<sup>4</sup>

As a result, the harms that we identified in our initial filings continue to persist, and they will continue for as long as these practices exist. The presence of the exemption is an integral piece of continuing to guide security practices in directions that align with best practices and benefit consumer protection and national security. As the Register recently explained "[b]ecause it has become clear that there is a need for good-faith security researchers to access computer programs and TPMs protecting copyrighted works, the Office recommends that Congress expand the kinds of activities that a security researcher is permitted to perform under sections 1201(j)(1) and 1201(j)(3)(A)"<sup>5</sup> and "the Office... continues to believe that the exemption adopted in 2015 can be a useful starting point."<sup>6</sup> Given that Congress has not yet acted on the Office's recommendation and that the need for the exemption continues to exist, we request that the exemption be renewed.

---

<sup>1</sup> <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/>

<sup>2</sup> <https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/>

<sup>3</sup> <https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm>

<sup>4</sup> <https://medsec.com/entries/stj-lawsuit-response.html>

<sup>5</sup> <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf>, p.75

<sup>6</sup> <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf>, p.74

## Item D. Declaration and Signature

The declaration is a sworn statement made under penalty of perjury, and must be signed by one of the petitioners named above.

**I declare under penalty of perjury under the laws of the United States of America that the following is true and correct:**

- 1. Based on my own personal knowledge and experience, I have a good faith belief that but for the above-selected exemption's continuation during the next triennial period (October 2018 – October 2021), technological measures controlling access to relevant copyrighted works are likely to diminish the ability of relevant users to make noninfringing uses of these works, and such users are likely to rely upon the above-selected exemption during the next triennial period.**
- 2. To the best of my knowledge, there has not been any material change in the facts, law, or other circumstances set forth in the prior rulemaking record (available at <https://www.copyright.gov/1201/2015>) that originally demonstrated the need for the above-selected exemption, such that renewal of the exemption would not be justified.**
- 3. To the best of my knowledge, the explanation provided in Item C above is true and correct, and supports the above statements.**

**Name/Organization:**

*If the petitioner is an entity, this declaration must be signed by an individual at the organization having appropriate personal knowledge.*

Signature: /s/ Andrea Matwyshyn

On behalf of

The Security Researchers

*This declaration may be signed electronically (e.g., "/s/ John Smith").*

Date: July 31, 2017