Before the
U.S. Copyright Office
Library of Congress

In the Matter of	Docket No. 2015-8
Public Study to Assess the Operation of Section 1201 of Title 17, Including the Triennial Rulemaking Process	80 Fed. Reg. 81,369

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Summary

New America's Open Technology Institute ("OTI") respectfully files these comments in response to the Copyright Office's Notice of Inquiry and Request for Public Comment concerning its public study into the efficacy of Section 1201 of the Digital Millennium Copyright Act (17 U.S.C. 1201).[1] OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multi-disciplinary approach that brings together advocates, researchers, organizers, and innovators.[2]

We thank you for the opportunity to comment on Section 1201 of the Digital Millennium Copyright Act (DMCA) as you undertake a study of its efficacy. We believe

[1] Section 1201 Study, *Notice of Inquiry and Request for Public Comment*, 80 Fed. R. 81,369 (Dec. 29, 2015), *available at* http://copyright.gov/fedreg/2015/80fr81369.pdf.
[2] New America's Open Technology Institute, https://www.newamerica.org/oti/.

Section 1201 of the DMCA has failed to protect creators and innovators and has instead been used to stifle competition in the marketplace. Additionally, it has thrown up roadblocks for individuals who wish to use and alter products that they own in a manner that will maximize their enjoyment and accessibility. Finally, it has chilled the critical work of researchers who seek to identify security vulnerabilities and ensure that the products upon which our lives increasingly depend are safe, reliable, and less vulnerable to malicious attacks.

This comment responds to the following subjects of inquiry posed by the Copyright Office, and lays out the ways in which Section 1201 should either be amended by Congress or reinterpreted by the Copyright Office in order to address those concerns:

A. Inquiry 1: Section 1201(a) has been ineffective in accomplishing its intended purpose of supporting marketplace competition and fostering innovation by protecting creators' rights.
B. Inquiry 2: The Copyright Office should apply a presumption in favor of exemptions under Section 1201 to establish interoperability or to enhance security research.
C. Inquiry 3: Section 1201 should be adjusted to apply a presumption in favor of renewal of previously granted exemptions.
D. Inquiry 4: In determining whether a proponent of an exemption has met the legal requirements set forth under Section 1201, the Copyright Office should define "adverse effects" narrowly, consistently require a finding that a request

is "likely" noninfringing, and establish a way to submit confidential versions of comments.

E. Inquiry 8: Reforms are needed to expand the scope of exemptions under Section 1201 for encryption research and security testing.

A. Inquiry 1: Section 1201(a) has been ineffective in accomplishing its intended purpose of supporting marketplace competition and fostering innovation by protecting creators' rights, and instead has suppressed marketplace competition.

When Congress passed the DMCA, it explained that the intent of Section 1201 was to support competition in the marketplace by establishing copy protections so that people could not interfere with creators' ability to profit off of their works by proliferating pirated copies of their creations, which would thereby create a disincentive for creators to publish new works.[3] Unfortunately, instead of fostering new innovation and marketplace competition, Section 1201 has often been used as a tool to stymie it by suppressing the attempts of competitors to join the marketplace. There are numerous examples of companies using Section 1201 for this type of anti-competitive behavior, which often targeted enforcement on products that were only tangentially copyrighted material, such as when Lexmark printers sued a third party to prevent them from competing for sales of printer cartridges[4]; or when a manufacturer of garage door openers sued to prevent

[3] Report of the H. Comm. on Judiciary on the Digital Millennium Copyright Act of 1998, H.R. Rep. No. 105-551, pt. 1, at 9–10 (1998) [hereinafter Judiciary Comm. DMCA Report].

[4] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

Skylink from selling a universal transmitter that was compatible with their products[5]; and when Microsoft sued a chip manufacturer to prevent it from selling third party accessories for the Xbox 360.[6]

Further, the DMCA is not completely effective at preventing piracy; the more effective tool against the proliferation of infringing digital copies seems to have been extensive innovation in new and increasingly easy-to-use legal ways to license or purchase copies of works. For example, at least one study has found that approximately 46% of Americans engage in some form of digital "piracy," but often times those who do also purchase more digital media through legitimate means.[7]

Even with remaining piracy, creators like those in the gaming and film industries continue to make billions of dollars every year. In 2014, the U.S. gaming industry earned $15 billion in revenues and is projected to earn $19.6 billion in 2019 (a 30% increase).[8] The Entertainment Software Association, a major trade association representing the gaming industry, boasts that the U.S. gaming industry is one of nation's fastest growing

[5] Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004).

[6] Datel Holdings, Ltd. v. Microsoft Corp., 2010-2 Trade Cas. (CCH) P77, 192 (N.D. Cal. 2010). *See also* Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (Storage Technology, a storage solution vendor, sued the independent vendor Custom Hardware Engineering in order to suppress market competition for aftermarket maintenance of its products).

[7] Joe Karaganis & Lennart Renkema, *Copy Culture in the US and Germany*, 5, American Assembly at Columbia Univ. (2013), *available at* http://piracy.americanassembly.org/wp-content/uploads/2013/01/Copy-Culture.pdf; see Comments of Organization for Transformative Works at pp. 1–2.

[8] Dean Takahashi, *U.S. games industry forecast to grow 30 percent to $19.6B by 2019*, Venture Beat (June 2, 2015), http://venturebeat.com/2015/06/02/u-s-games-industry-forecast-to-grow-30-to-19-6b-by-2019/.

industries.[9] The movie industry earns approximately $10 billion per year in the U.S. alone.[10]

Finally, much of the infringement that does still occur and significantly impacts U.S. businesses is often committed by non-U.S. actors, such as by counterfeit producers in China and Russia.[11] Indeed, by amending the DMCA and reforming how the Copyright Office applies the law so that it favors security research, the experts and researchers who are now chilled in their attempts to identify and patch security vulnerabilities may be able to join the front lines in stopping international intellectual property theft by helping creators to enhance the security of their products and protect them against breaches by malicious actors.

B. Inquiry 2: The Copyright Office should apply a presumption in favor of exemptions under Section 1201 to establish interoperability or to enhance security research.

[9] Entertainment Software Association, *Games: Improving the Economy* (Nov. 2014), http://www.theesa.com/wp-content/uploads/2014/11/Games_Economy-11-4-14.pdf.

[10] MPAA, *Theatrical Market Statistics* (2014), http://www.mpaa.org/wp-content/uploads/2015/03/MPAA-Theatrical-Market-Statistics-2014.pdf. Though the movie industry is experiencing struggling sales, that drop is attributed primarily to demographic shifts, accessibility of new media for viewers like streaming and mobile applications, and even the excessive costs of tickets and refreshments, among a plethora of other factors, none of which are related to piracy. *See* Max Willens, *Box Office Ticket Sales 2014: Revenues Plunge To Lowest In Three Years*, Int'l Business Times (Jan. 5, 2015), http://www.ibtimes.com/box-office-ticket-sales-2014-revenues-plunge-lowest-three-years-1773368; Erich Schwartzel & Ben Fritz, *Fewer Americans Go to the Movies: Theater Owners Consider Cutting Ticket Prices One Day a Week*, Wall St. J. (Mar. 25, 2014), http://www.wsj.com/articles/SB10001424052702303949704579461813982237426. ; *and* Roger Ebert, *I'll Tell You Why Movie Revenue Is Dropping*, Roger Ebert's J. (Dec. 28, 2011), http://www.rogerebert.com/rogers-journal/ill-tell-you-why-movie-revenue-is-dropping.

[11] Amb. Michael B.G. Froman, U.S. Trade Rep., *2015 Special 301 Report*, Exec. Office of the President (2015), *available at* https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf.

The Copyright Office should apply a presumption in favor of granting proponents' requests for exemptions to establish interoperability or to enhance security research. When someone purchases a product, they should be able to alter it in any way they see fit, so long as it is not in order to intentionally infringe upon a creator's copyright.

The presumption in favor of granting an exemption should extend, in particular, to proposed exemptions to establish interoperability with other products, regardless of whether the producer has established a protective measure in an attempt to ensure that consumers only use that product with other products that are within the suite of the producer's offerings. Without these important exemptions, Section 1201 not only interferes with one's freedom to control and enjoy their property, it also undermines market competitiveness by limiting consumer choice and blocking other potential innovators from entering that market, as was the case in the lawsuits cited in the previous section.

Additionally, the Copyright Office should apply a presumption in favor of granting proponents' requests for exemptions when they apply to security research, including those that could impact public safety. Now more than ever before, devices large and small are run by computers or are connected to the Internet, and are thus potential targets of malicious attacks. OTI has previously commented at length about the importance of security research as it relates to connected medical devices.[12] Additionally, car safety serves as a particularly salient example of how security research can implicate public safety. Last year's now-infamous Jeep-hacking experiment—where security researchers

[12] Laura Moy, *Class 25 and Class 27 Reply Comments*, Docket No. 2014-07, New America's Open Technology Institute 5 (May 1, 2015), https://static.newamerica.org/attachments/4448-why-copyright-law-is-undermining-cybersecurity-and-how-to-fix-it/ReplyComments_LongForm_OTI_Class25.92dc248a9ac94e4286787af4f6ce3dcc.pdf.

remotely accessed the car's air-conditioning, radio, and windshield wipers, and even cut the transmission and stopped it on a highway[13]—may be the most prominent example of why this kind of research is essential to product safety and public safety, but it will certainly not be the last.

Instead of leading to a push to expand these kinds of research opportunities for security experts, the Jeep experiment inspired a bill in the House of Representatives that would criminalize it.[14] Since then, a scandal involving Volkswagen exposed the car manufacturer's purposeful and successful attempt to evade emissions standards by deploying code on 11 million of its vehicles that reduced those cars' emissions while they were being tested.[15]

Cases such as these will only increase as more devices and machines are run by computers and are connected to the Internet, making independent research such as the kind that identified the Jeep vulnerability, or that might have identified the Volkswagen scam, more essential than ever before.

C. Inquiry 3: Section 1201 should be adjusted to apply a presumption in favor of renewal of previously granted exemptions.

[13] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (Jul. 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[14] Harley Geiger, *Draft Car Safety Bill Goes Too Far*, Center for Democracy & Tech. (Oct. 20, 2015), https://cdt.org/blog/draft-car-safety-bill-goes-in-the-wrong-direction/.
[15] Karl Russell, Guilbert Gates, Josh Keller, & Derek Watkins, *How Volkswagen Got Away With Diesel Deception*, NY Times (Jan. 5, 2016), http://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html?_r=0.

It is our opinion that Section 1201 of the DMCA does not require the Copyright Office to examine exemption proposals "de novo" every three years.[16] But because the Copyright Office nevertheless insists on examining proposed exemption renewals de novo, Congress should amend DMCA Section 1201 to require a presumption in favor of renewing previously granted exemptions.

A presumption in favor of renewing previously granted exemptions would provide a badly-needed basis for those who rely on exemptions to have confidence that the exemptions are stable. Security research often takes many years to bear fruit, but the current exemption period is limited to three years, and in some instances, such as with research on vehicles, that period of time can be even shorter.[17] Some researchers choose to forgo particular types of work that may have had great public value out of fear that they may not be able to prove the value of their work and the need for their exemption to be renewed once expired.

Congress and the Library of Congress (LOC) should work together to address this problem. The DMCA should encourage long-term research, and the LOC should automatically renew any previously granted or renewed exemption unless an opponent of its renewal offers new and compelling evidence that shows a material change in

[16] The statute is silent on the question of whether or not review should be conducted de novo. In applying a de novo standard, the Copyright Office has cited to a single House Commerce Committee Report on a draft version of the DMCA. See *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Notice of Inquiry and Request for Petitions, 79 Fed. Reg. 55687, 55689 (Sept. 17, 2014) (citing *Report of the H. Comm. on Commerce on the Digital Millennium Copyright Act of 1998*, H.R. Rep. No. 105-551, pt. 2, at 37 (1998)). The Copyright Office arguably has the interpretive authority to adopt a different standard of review.

[17] Final Rule, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Librarian of Cong., Docket No. 2014-07, P. 50 (Oct. 2015), http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf.

circumstances such that the lack of an exemption would not harm or adversely affect users or consumers, and that the exemption has negatively impacted the value or the market for the underlying work. If the LOC makes this finding, then the renewal of that exemption should be subject to the same review as new exemption requests.

Establishing a presumption in favor of renewal and imposing the burden of proof showing why the exemption should not be renewed on its opponent would relieve security researchers of the costly regulatory process and of the uncertainty that their work may be halted before completion.

D. Inquiry 4: In determining whether a proponent of an exemption has met the legal requirements set forth under Section 1201, the Copyright Office should define "adverse effects" narrowly, consistently require a finding that a request is "likely" noninfringing, and establish a way to submit confidential versions of comments.

Currently, the Copyright Office interprets the DMCA to place more of a burden on proponents of an exemption than Congress intended or than the letter of the law requires. In reviewing exemptions, the Copyright Office should define "adverse effects" narrowly and consistent with the statute. In previous comments, OTI urged the Copyright Office to define "adverse effects" narrowly, referring only to an inability to make a noninfringing use. We argued that:

> [T]he concerns that gave rise to this rulemaking were widespread use of [technological protection measures (TPM)] across entire classes of works, and the use of TPM to enforce business models rather than to defeat piracy. Combining the crystal clear language of the statute with legislative history, an "adverse effects" inquiry should be simple: Does or will widespread use of TPM and/or the use of TPM for purposes other than the prevention of piracy diminish users' ability to make uses that are likely noninfringing? …
>
> The law is concerned only with the inability to make a use that is likely noninfringing. Outside the context of a fair use inquiry that the Copyright Office may need to perform to determine whether or not the desired use is noninfringing, §1201 is not concerned with a user's motivation for making a First-Amendment-protected lawful use, or with secondary harms "stemming from" the inability to make that use.[18]

In addition to adopting a narrow definition of "adverse effects," the Copyright Office should consistently require a determination that the proposed use is "likely noninfringing" to support granting an exemption. As we noted in the same previous comments, the Copyright Office has at times required far more certainty that a proposed use is noninfringing than a showing that it is likely or probably noninfringing.[19] By consistently applying the requirement for a determination that a use is "likely

[18] Laura Moy, Comments In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Docket No. 2014-07), New America's Open Technology Institute, Feb. 6, 2015, https://static.newamerica.org/attachments/4448-why-copyright-law-is-undermining-cybersecurity-and-how-to-fix-it/InitialComments_LongForm_NAOTI.8af57d9703e646eebe6a76d4013d8c71.pdf.
[19] Id. at 7.

noninfringing," the Copyright Office would be acting in a manner consistent with the statute and would lessen an unnecessary burden on security researchers and others who seek to make fair use of their products and devices.

Finally, in those previous comments we recommended that the Copyright Office allow proponents of exemptions to submit confidential versions of their comments if they are able to demonstrate a need to do so. We noted that the need for such a mechanism stems from the concern that:

> [s]ome information that could be critical to the decision-making process is not appropriate for public disclosure because, for example, it is business-confidential, it might expose commenters to legal liability, or it would disclose security vulnerabilities that could then be exploited by malicious third parties.
>
> The absence of a mechanism for submission of confidential comments is particularly problematic for security researchers. One of the reasons security researchers request exemptions in every triennial review is because the threat of legal liability under §1201 sometimes prevents them from publishing important work. The same fear of legal liability could prevent them from filing public comments in this rulemaking detailing the important work that they do.[20]

[20] Id. at 8-9.

Thus, creating a mechanism for confidential filings would address a legitimate need that would help to ensure a more complete record in the Copyright Office's proceedings. It would also be in keeping with the practices of other federal agencies, like the Federal Communications Commission, which allows for confidential filings in certain circumstances.

E. Inquiry 8: Reforms are needed to expand the scope of exemptions under Section 1201 for encryption research and security testing.

The current applications of "encryption research" and "security testing" under the DMCA are too narrow and should be broadened in the statute. Currently, the activities of security researchers are chilled out of fear that they will be pursued criminally and civilly under the DMCA or other statutes like the Computer Fraud and Abuse Act.[21] Amending the DMCA to make clear that a broad swath of encryption research and security testing does not constitute a violation of Section 1201 will release a major pressure valve for researchers that currently stops their efforts in their tracks and that leaves us all more vulnerable to attack.

Two bills have been introduced this Congress that would reform the DMCA and address these concerns to varying degrees. The Unlocking Technology Act of 2015 (H.R. 1587) would offer the most robust reforms because it would make clear that circumvention of TPMs is only a violation under the DMCA if "the purpose of such circumvention" is to

[21] Statement from 49 security, policy, and academic experts on Legal Impediments to Cybersecurity Research (May 1, 2015, *updated* May 21, 2015), http://www.ischool.berkeley.edu/files/cybersecurity-statement-rev9.pdf.

engage in copyright infringement.[22] This bill would also remove prohibitions against unlocking cell phones or other mobile devices by authorizing a device owner or a party with the owner's consent to "adapt the software or firmware … to connect to a wireless communications network."[23] Thus, this bill would remove all uncertainty from the activities of security researchers, hobbyists, tinkerers, and users by ensuring that only acts to purposefully infringe upon another's copyrighted work constitute violations of the DMCA.

The second bill, the Breaking Down Barriers to Innovation Act of 2015 (H.R. 1883), takes a more circumspect approach to DMCA reform. It tasks the LOC with ensuring that noninfringing uses of copyrighted works are not "unduly burdened" and with seeking a balance between enabling people to "make noninfringing use of copyrighted works and the legitimate protection of intellectual property rights."[24]

While this bill does not go so far as the Unlocking Technology Act to make all noninfringing uses permissible under Section 1201, it would significantly improve upon its current application by ensuring that the LOC's analysis favors granting exceptions more and relieves the proponent of an exemption from bearing burden of proof. It would also relieve exemption proponents of the constraints and some of the chilling effect associated with the three year review process by empowering the LOC to conduct rulemakings

[22] Unlocking Technology Act, H.R. 1587, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1587/text.
[23] Id.
[24] Breaking Down Barriers to Innovation Act of 2015, H.R. 1883, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1883/text.

outside of that schedule, and by creating a presumption of renewal, as we urged should be adopted in Part C of this comment.[25]

These kinds of statutory reforms are not only supported by a wide range of civil society groups and experts,[26] they are also fast becoming an urgent priority for our cybersecurity and our national security. Not only are we living in a world where HVAC systems can be a malicious attackers' point of entry into payment systems, as was likely the case in the Target hack,[27] it is one where everything[28] from cars,[29] airplanes,[30] and

[25] Id.

[26] *See e.g.* Press Release, *Public Knowledge Welcomes Sen. Wyden's Proposal to Reform Digital Millennium Copyright Act*, Public Knowledge (Apr. 16, 2015), https://www.publicknowledge.org/press-release/public-knowledge-welcomes-sen-wydens-proposal-to-reform-digital-millennium; Letter from Erik Stallman, Dir. Open Internet Project, Ctr. for Democracy & Tech., to Rep. Jared Polis (Apr. 17, 2015), https://cdt.org/files/2015/04/CDT-letter-of-support-for-HR-1883.pdf; Stan Adams, *Thawing Chilled Security Research: An Opportunity for the Copyright Office*, Ctr. for Democracy & Tech. (May 5, 2015), https://cdt.org/blog/thawing-chilled-security-research-an-opportunity-for-the-copyright-office/; Parker Higgins, *New Bipartisan Bill Proposes Real Fixes to Bad Copyright Law*, Electronic Frontier Foundation (May 9, 2013), https://www.eff.org/deeplinks/2013/05/new-bipartisan-bill-proposes-real-fixes-bad-copyright-law; Mitch Stolz, *New "Breaking Down Barriers to Innovation Act" Targets Many of DMCA Section 1201's Problems*, Electronic Frontier Foundation (Apr. 20, 2015), https://www.eff.org/deeplinks/2015/04/new-breaking-down-barriers-innovation-act-targets-many-dmca-section-1201s-problems; *and* Press Release, *Library Copyright Alliance Applauds Introduction of the Barriers to Innovation Act*, American Library Ass'n (Apr. 17, 2015), http://arllca.nonprofitsoapbox.com/storage/documents/lca-barriers-legislation.pdf.

[27] Brian Krebs, *Target Hackers Broke in Via HVAC Company*, Krebs on Security (Feb. 14, 2015), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[28] Marilyn Cohodas, *4 IoT Cybersecurity Issues You Never Thought About*, DarkReading (Sept. 24, 2015), http://www.darkreading.com/endpoint/4-iot-cybersecurity-issues-you-never-thought-about-/a/d-id/1322330.

[29] *Supra* note 13.

[30] Kim Zetter, *Feds Say That Banned Researcher Commandeered a Plane*, Wired (May 15, 2015), http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

medical devices[31] to tv sets[32] can be hacked. Forecasters predict that the Internet of Things (IoT) will grow rapidly, turning into a multi-trillion-dollar market in the next decade.[33]

The rapid expansion of IoT increases the risk of data breaches that we currently face, and introduces significant new types of risks as well. National security experts have now joined security researchers in cautioning how grave a threat IoT poses to cybersecurity and national security. Last month, the Director of National Intelligence testified before the Senate and House Intelligence Committees during Worldwide Threats briefings that cybersecurity threats associated with the broad adoption of IoT "can threaten data privacy, data integrity, or continuity of services."[34]

Given the seriousness of these threats, it is incumbent upon Congress to undertake statutory reforms like the Unlocking Technology Act or the Breaking Down Barriers to Innovation Act which would thaw some of the chill that currently prevents security researchers from undertaking efforts to identify and fix security vulnerabilities that pose threats to public safety, privacy, the economy, and national security.

---

[31] Jerome Radcliffe, Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System, Black Hat USA (2011), https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

[32] SeungJin Lee & Seungjoo Kim, *Hacking, Surveilling, and Deceiving Victims on Smart TV*, BlackHat USA (2013), https://media.blackhat.com/us-13/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf.

[33] James Manyika, et. al, *Unlocking the Potential of the Internet of things*, McKinsey (June 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[34] *See Worldwide Threats, Hearing before the U.S. Senate Select Comm. on Intelligence*, 114th Cong. (Feb. 9, 2016) (written statement of Dir. of Nat'l Intelligence James Clapper); *and See Worldwide Threats, Hearing before the House Permanent Select Comm. on Intelligence*, 114th Cong. (Feb. 25, 2016) (written statement of Dir. of Nat'l Intelligence James Clapper), *available at* http://docs.house.gov/meetings/IG/IG00/20160225/104550/HHRG-114-IG00-Wstate-ClapperJ-20160225.pdf.

Conclusion

While the DMCA is not the only law that chills this crucial work, its anti-circumvention provisions in Section 1201 do present a major obstacle. As described throughout this comment, OTI believes that the Copyright Office and Congress have both the power and the means to enact necessary reforms. We thank the Copyright Office for providing us with the opportunity to submit comments on this critically important issue.

Respectfully submitted,

/s/

Robyn Greene
Policy Counsel
New America's Open Technology Institute
Washington, DC 20001
(202) 596-3609

Filed: March 3, 2016