# Petition for Proposed Exemption Under 17 U.S.C. § 1201

## Item 1. Submitter and Contact Information

The submitters are a group of academic security researchers comprised of Prof. Steven M. Bellovin (Columbia University), Prof. Matt Blaze (University of Pennsylvania), Prof. Edward W. Felten (Princeton University), Prof. J. Alex Halderman (University of Michigan), and Prof. Nadia Heninger (University of Pennsylvania) (the "Submitters").

## Item 2. Brief Overview of Proposed Exemption

Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when

(a) circumvention is accomplished for the purpose of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measure or the underlying work it protects; OR

(b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder fails to comply with the standards set forth in ISO 29147 and 30111; or (2) the finder of the malfunction, security flaw or vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder by providing the information set forth in Form A* in advance of or concurrently with public dissemination of the security research.

* Form A includes the information referenced in ISO 29147 Annex A

## Item 3. Copyrighted Works Sought to be Accessed

"Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities"

This delineation builds on the following two previously-granted exemptions (relevant portions in italics):

- The 2000 exemption for "*Literary works, including computer programs and databases, protected by access control mechanisms that* fail to permit access *because of malfunction,* damage, or obsoleteness."
- The 2006 exemption for "Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit *security flaws or vulnerabilities* that compromise the security of personal computers, *when circumvention is accomplished* solely *for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities*" (the "2006 Audio Security Research Exemption").

## Item 4. Technological Protection Measure

Any TPM and its underlying computer code that may contain a malfunction, security flaw or vulnerability potentially exposes the public to increased risk of harm. Such harms may include, without limitation, serious physical injury or death of natural persons, individually or en masse, property damage or financial harms.

Examples of such TPMs and computer code include, but are not limited to, the TPMs and computer code in (1) insulin pumps, pacemakers and other medical devices, such as those controlling dosing or other device behavior; (2) car components, such as the computer code that controls braking and acceleration systems; (3) SCADA systems and other critical infrastructure, such as the computer code that controls nuclear power plants, smartgrids, and industrial control systems; (4) smartphones that operate critical applications such as health or safety-critical applications, such as pacemaker applications; (5) internet-enabled consumer goods in the home, such as digital smoke alarms or carbon monoxide detectors; and (6) transit systems, such as the computer code in air traffic control systems, train systems and traffic lights.

## Item 5. Noninfringing Uses.

The specific noninfringing use is the one articulated in the 2006 Audio Recording Security Research Exemption: circumvention is accomplished for the purpose of good faith testing, investigating, or correcting malfunctions, security flaws or vulnerabilities, as well as the circumvention that was part of an investigation that resulted in the public dissemination of security research regarding malfunctions, security flaws or vulnerabilities. The work will be used by security researchers in order to (a) unlock public access to knowledge about security research through conference presentations and publications in academic journals and proceedings; (b) improve safety of products and services relying on computer code; (c) improve national security of critical infrastructure relying on computer code; and (d) enable companies to perform and access security research as part of their legitimate business operations in order to create better products. Internet of things startups in particular face challenges in obtaining and affording security testing of their products.

Further, a close reading of DMCA Section 1201(i) demonstrates that Congress specifically contemplated and sought to protect the public from malfunctioning, flawed or vulnerable code that harms consumers: Section 1201(i) states that a consumer's investigation of code functionality on a privately-owned system in order to determine whether a privacy harm is happening does not constitute an impermissible circumvention. In this spirit of 1201(i), this exemption request similarly seeks to empower consumers with better information about how computer code is behaving on their systems and the systems upon which their safety relies. However, unlike 1201(i), this exemption request recognizes the practical reality that most consumers lack the technological skills needed to engage in the type of technical inquiry 1201(i) expressly authorizes. This exemption request, therefore, empowers security researchers to unlock the truth of code behaviors, acting as agents on behalf of the consumers suffering the harms contemplated by 1201(i) and other malfunctions, security flaws or vulnerabilities that expose the public to risk of harm.

## Item 6. Adverse Effects.

The immediate adverse effect of the TPMs is that Submitters have chosen not to perform specific acts of security research that they believe would have prevented harms to and benefited safety of human persons. Consequently, the Submitters have failed to produce and share the results of this research with the public. They perceive the DMCA to penalize the creation of potentially life-saving security research. Further, the Submitters have felt forced to delay the release of performed research regarding malfunctions, security flaws and vulnerabilities because of copyright holders' ability to pursue injunctions for the purpose of permanently suppressing disclosure of Submitters' research.[1] While the full extent of the opportunity cost of these failure and delays is unknowable at present, the Submitters believe that the unperformed research will unearth serious vulnerabilities in the target systems that are equivalent to or greater in severity to a large number of already discovered malfunctions, security flaws or vulnerabilities.[2] The Submitters also believe this unperformed research will yield evidence of the same types of adverse effects as currently known malfunctions, security flaws and vulnerabilities. These categories of adverse effect from known malfunctions, security flaws or vulnerabilities include, but are not limited to, past and expected future instances of:

1. Death or physical harms to human persons from malfunctions, security flaws or vulnerabilities in (a) medical devices and machines including radiation machines,[3] insulin pumps,[4] and

[1] Copyright litigation has been criticized for censorship of truthful speech, with plaintiffs sometimes suing to silence speech that criticizes their products. *See* Elizabeth Rowe, *Trade Secret Litigation and Free Speech: Is it?...*, 50 B.C. L. REV. 1425, 1444 (2009).

[2] The below-referenced examples of serious malfunctions, security flaws and vulnerabilities are from the last three years in most cases.

[3] At least six people died or were seriously injured due to a software malfunction, security flaw or vulnerability in the Therac 25 radiation machine. *See* Nancy Leveson, Clark Turner, *An Investigation of the Therac 25 Accidents*, , IEEE COMPUTER, July 1993, at 18, *available at* http://courses.cs.vt.edu/professionalism/Therac_25/Therac_1.html.

[4] *See, e.g.*, Jordan Robertson, *McAfee hacker says Medtronic insulin pumps vulnerable to attack*, BLOOMBERG (Feb. 29, 2012, 10:00 AM) http://www.bloomberg.com/news/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack.html. For technical specifications regarding insulin pump vulnerabilities, *see, e.g.*, 95762*: Medtronic Multiple Unspecified Insulin Pumps Serial Number Information Disclosure*, OSVDB, http://www.osvdb.org/show/osvdb/95762 (last visited Nov. 3, 2014); 95761*: Medtronic Multiple Unspecified Insulin Pumps Warning Disabling Weakness*, OSVDB, http://www.osvdb.org/show/osvdb/95761 (last visited Nov. 3, 2014).

pacemakers;[5] (b) cars and car components;[6] and (c) other machines and consumer products.[7]

2. Damage to property and national security interests, potentially leading to death and physical harms to human persons from malfunctions, security flaws or vulnerabilities in (a) smartgrids;[8] (b) power and water stations;[9] (c) air traffic control systems[10] and other communication systems;[11] (d) health systems;[12] (e) nuclear power plants;[13] and (f) compromised networks of

[5] *See, e.g.*, Andrea Peterson, *Yes Terrorists Could Have Hacked Dick Cheney's Heart,* WASH POST (Oct. 21, 2013) http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/. For technical specifications regarding pacemaker vulnerabilities, *see, e.g.*, 87034*: Multiple Unspecified Implantable Cardioverter Defibrillator (ICD) Remote Unspecified Backdoor*, OSVDB, http://www.osvdb.org/show/osvdb/87034 (last visited Nov. 3, 2014).

[6] A jury determined a malfunction, security flaw or vulnerability in car software to have been involved in the death of one senior citizen and the serious injury of another. *See Jury Finds Toyotal Liable in Defective Accelerator Case*, KLTV http://www.kltv.com/story/23790635/jury-finds-toyota-liable-in-defective-accelerator-case (last visited Nov. 3, 2014). For additional examples of known car vulnerabilities *see, e.g.*,113619*: Tesla Model S Unspecified Remote Compromise*, OSVDB http://www.osvdb.org/show/osvdb/113619 (last visited Nov. 3, 2014); 81567: Car Portal CMS File Upload PHP Code Execution, OSVDB, http://www.osvdb.org/show/osvdb/81567 (last visited Nov. 3, 2014); 102990: Toyota Camry Engine Control Module (ECM) Multiple Unspecified Race Conditions, OSVDB, http://www.osvdb.org/show/osvdb/102990 (last visited Nov. 3, 2014).

[7] *See* David Goldman, *Shodan: The scariest search engine on the Internet,* CNN (April 8, 2013: 1:41 PM) http://money.cnn.com/2013/04/08/technology/security/shodan/.

[8] *See, e.g.*, 104688*: Multiple Unspecified Advanced Metering Infrastructure (AMI) Port Scan Remote DoS*, OSVDB, http://www.osvdb.org/show/osvdb/104688 (last visited Nov. 3, 2014).

[9] *See* Kim Zetter, *Researchers Uncover Holes That Open Power Stations to Hacking*, WIRED (Oct. 16, 2013, 12:00 PM) http://www.wired.com/2013/10/ics/.

[10] *See* Heather Kelly, *Researcher: New Air Traffic Control System is Hackable*, CNN TECH (July 26, 2012, 6:49 PM), http://www.cnn.com/2012/07/26/tech/web/air-traffic-control-security.

[11] *See* U.S. COMPUTER EMERGENCY RESPONSE TEAM, POTENTIAL VULNERABILITIES IN MUNICIPAL COMMUNICATIONS NETWORKS (2006), *available at* http://www.us-cert.gov/control_systems/pdf/Potential_Vulnerabilities_Municipal_Communications_Networks_v1.pdf.

[12] *See, e.g.*, Dan Kaplan, *Indiana University Hospital Hacked to Steal Data*, SC MAG. DATA BREACH BLOG (Feb. 1, 2012), http://www.scmagazine.com/indiana-university-hospital-hacked-to-steal-data/article/225887/.

[13] *See* Andy Greenberg, *America's Hackable Backbone*, FORBES (Aug. 22, 2007, 6:00 PM), http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html.

personal computers[14] and smartphones[15] that can be repurposed for attacking critical national assets.

3. Damage to innovation, progress of science and useful arts, consumer trust, and the growth of the economy of the United States. The Submitters further believe that stifling security research materially undermines the innovation policy of the United States and materially hinders the progress of science and useful arts. In addition to academic and private sector individual researchers, responsible companies are themselves engaging in security research into other companies' products in order to safely interoperate with them. Reports of malfunctions, security flaws and vulnerabilities now frequently come from one company to another.[16] In particular, the companies signing the following petition have expressed concern over the current legal uncertainty surrounding security research under the DMCA and believe it to be actively damaging their businesses and the future of U.S. innovation: https://www.c4sr.org/#petition.

Our society now trusts computer code to run many aspects of our economy, including our stock markets, which we know to have been recently compromised.[17] Independent security research into the integrity of computer code helps protect the public from code that contains malfunctions, security flaws or vulnerabilities. While responsible copyright holders test their code for errors, not all errors are known at the time of release.[18] Removing DMCA barriers to security research through this exemption benefits the public without altering any of the numerous other legal remedies copyright holders have at their disposal. Independent security research is a technological audit mechanism that is critical to stimulating improvements in the safety of computer code and preserving public trust in U.S. innovation policy and our economy. It also stimulates a more balanced social discourse around the costs and benefits of particular new technologies and the best direction for innovation policy in the United States.

---

[14] *See* Andy Greenberg, *Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks,* WIRED (Sept. 25, 2014, 4:49 PM) http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/.

[15] *See* Steven J. Vaughan-Nichols, *First Case of Android Trojan Spreading via Mobile Botnets Discovered*, ZDNET (Sept. 5, 2013, 16:33 GMT) http://www.zdnet.com/first-case-of-android-trojan-spreading-via-mobile-botnets-discovered-7000020292/.

[16] *See, e.g.,* Adrianne Jeffries, *Google Engineers Found Over Half the Bugs in Microsoft's Latest Security Update,* THE VERGE (Feb. 13, 2013, 9:00 am) http://www.theverge.com/2013/2/13/3983846/googlers-found-over-50-percent-of-the-bugs-in-microsofts-massive-update.

[17] *See* Michael Riley, *How Russian Hackers Stole the Nasdaq*, BLOOMBERG BUSINESSWEEK (July 17, 2014) http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

[18] Also, some less responsible copyright holders refuse to correct serious, known vulnerabilities, even when demands for correction come directly from government bodies. *See, e.g.,* Advisory ICSA-14-084-01, US-CERT, *available at* https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01 (stating that the vendor "has decided not to resolve these vulnerabilities, placing critical infrastructure asset owners using this product at risk.").