Intellectual Property Brief

Volume 9 | Issue 1 Article 1

2018

How the Digital Millennium Copyright Act Affects Cybersecurity

Katherine Weigle
National Hospitality Group

How the Digital Millennium Copyright Act Affects Cybersecurity

HOW THE DIGITAL MILLENNIUM COPYRIGHT ACT AFFECTS CYBERSECURITY

Katherine Weigle[1]

ABSTRACT

Black hat hackers have been unlawfully accessing and controlling everything from vehicle software to medical implants; these dangerous and manipulative hacks can control and influence life-threatening software. In response to the threat, cybersecurity researchers are often unable to provide immediate, viable, and all-encompassing solutions to these security issues due to the danger of copyright infringement under the anti-circumvention exemptions of the Digital Millennium Copyright Act (DMCA). If Section 1201 of the DMCA continues to maintain an exemption for circumvention, security researchers will be able to circumvent technology and software to find safety glitches and reasonable alternatives—and thus foreshadowing or preventing hackers from unlawfully controlling these technologies.

Over the years, many researchers and security analysts have advocated that the U.S. Copyright Office should maintain a permanent exemption in the DMCA through the creation of new rules tailored explicitly to security research. Like other proposals, this article will address the problems being faced in the cybersecurity industry, but alternatively, will provide potential reform solutions as to how security researchers may circumvent technology without the fear of prosecution. This article will offer alternatives and discuss proposed amendments to the DMCA, and address the issue as to which governing authority should oversee the DMCA, as well as provide an analysis of the continuously changing anti-circumvention exemption. Through research and a comparison of past, present, and potential law, this article will weigh the pros and cons of amending the Section 1201 exemption for researchers, and discuss whether the U.S. Copyright Office is the appropriate governing authority to regulate the DMCA.

---

[1] Corporate Attorney, National Hospitality Group, LLC. LL.M. in intellectual property, American University Washington College of Law, 2017; J.D., Charleston School of Law, 2016; B.A., University of South Carolina, 2013. She would like to express her deepest gratitude to the staff of the American University Intellectual Property Brief for their tremendous work and care.

TABLE OF CONTENTS

ABSTRACT **1**

INTRODUCTION **3**

I. Security Research is Essential for Cybersecurity Development **6**

A. What is Cybersecurity? 7

B. How Cybersecurity Research Impacts Security Issues 8

II. Incomplete Protections in the DMCA **11**

A. History Behind the Library of Congress and U.S. Copyright Office 11

B. The DMCA and the 1201 Exemption 12

C. The DMCA's Restriction on Security Research 14

D. Opposition to Anti Circumvention Exemptions 16

III. Reform Solutions for Security Research **19**

A. Amending the Anti-Circumvention Exemptions 19

B. Should the U.S. Copyright Office Oversee the DMCA? 21

CONCLUSION: TOWARD THE FUTURE **23**

INTRODUCTION

Cybersecurity is arguably the most significant security concern for the United States. It functions to protect the United States and its citizens from dangerous and unauthorized attacks from computers, networks, software, and data. Security research is an essential component of cybersecurity practices and is utilized to detect security vulnerabilities in digital devices that could be targeted and exploited by hackers. Presently, the copyright infringement laws that protect these digital devices conflict with the efforts to conduct security research.[2]

The Digital Millennium Copyright Act (DMCA) was enacted by Congress in 1998[3] to prevent copyright infringement of digital copyrighted works; this was Congress' attempt to create copyright laws that specifically addressed new digital developments. Two treatises from the World Intellectual Property Organization were used as the basis for forming this legislation.[4]

A large portion of the DMCA focuses on anti-circumvention laws; these laws were intended to prevent copyright infringement by penalizing unauthorized users who circumvent or hack into copyrighted technology or software. Circumvention is similar to picking a lock on a door; to circumvent the software, users often have to break through access controls or technological protection measures (TPM)[5] that were put in place to protect the software itself from unauthorized users. The act of using circumvention software has often been considered to constitute a copyright infringement violation when it breaks into a protected area of a copyrighted work.[6]

Section 1201 of the DMCA encompasses anti-circumvention exemptions that allow the circumvention of software by users, as long as those users are acting in good faith.[7] Under 1201(g)[8] of the DMCA, a security research exemption allows

---

[2] *See* Maryna Koberidze, *The DMCA Rulemaking Mechanism: Fail or Safe?*, 11 WASH. J.L. TECH. & ARTS 211, 213 (2011) (debating whether security researchers should be allowed to break into electronic devices through circumvention).

[3] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat.2860 (1998) (creating legal punishments for copyright infringements of digital works).

[4] WIPO Copyright Treaty, Dec. 20, 1996, 2186 U.N.T.S. 121.

[5] James L. Davis, *Is Interoperability just for those who can hack it? The application of the DMCA Interoperability Exceptions in the Consumer Electronics Industry,* 2005 U. Ill. J.L. Tech. & Pol'y 141, 142 (2005).

[6] 17 U.S.C. § 1201(a)(1) (2015) (focusing on the ability to circumvent software or technology, and the implications of these actions as copyright infringement acts).

[7] *Id.*

[8] *Id.* at § 1201(a)(1)(C) (discussing permissible acts of encryption research under the DMCA, including circumvention of TPMs. 1201(g)(2) states "notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the

researchers to circumvent TPMs for good faith security research. However, this exemption has not been favored by security researchers due to the requirement that researchers must still seek and obtain permission from the copyright owner.[9] Many manufacturers and owners of the digital technology and software strongly disfavor any exemption for circumvention, since they believe permission could lead to abuse and misuse of the intellectual property.

Although DMCA exemptions are reviewed and potentially amended every three years by the Library of Congress[10] (based on reports received from the U.S. Copyright Office), many security researchers believe that the Library of Congress and U.S. Copyright Office are inhibiting cybersecurity research through these outdated circumvention regulations. For example, recent enforcement of the DMCA has caused legal implications for security researchers who were circumventing technology for good faith purposes.[11] This good faith research includes attempting to find security glitches and solutions in vehicle software and medical implants to prevent hackers from accessing the information and using it dangerously.[12] In 2015, the DMCA exemption was modified in favor of allowing circumvention of vehicle software and medical implants.[13] However, this modification has received criticism from digital copyright owners and agencies, stating that the exemption is indicative of a dangerous slope that can facilitate copyright infringement and hacks.[14]

The argument against allowing an anti-circumvention exemption, rests on whether good faith security research opens a dangerous door to abuse by other unauthorized users. Many vehicle manufacturers and agencies are arguing that

---

course of an act of good faith encryption research if--Use of technological means for research activities. Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to-- (A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph." *Id.* U.S.C. § 1201(g)(2) (2015) (discussing permissible acts of encryption research under the DMCA).

[9] *Id.*

[10] 17 U.S.C. § 1201(a)(1)(C). This review is considered to be a fail-safe for Congress which allows Congress to enforce circumvention prohibitions or grant them every three years. If a law is deemed unfavorable after three years, it grants Congress the option to review and amend the law.

[11] Eli Greenbaum, *No Country for Cybersecurity Arbitrage*, 34 Yale J. on Reg, 18, 20 (2016).

[12] Doctorow, Cory. *Pacemakers and Piracy: The Unintended Consequences of the DMCA for Medical Implants*. Electronic Frontier Foundation, 17 May 2016, www.eff.org/deeplinks/2016/04/pacemakers-and-piracy-why-dmca-has-no-business-medical-implants.

[13] *See* 37 C.F.R. § 201.40 (2015) (covering anti-circumvention exemptions). This regulation covers the new anti-circumvention exemptions, including allowing circumvention for good faith purposes, such as using on vehicle software. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies.

[14] *Id.*

allowing the exemption could enable individuals to take advantage of the vehicle technology and use it in an illegal manner, such as to violate emission laws. On the other hand, researchers who have circumvented vehicle technology for security purposes have found that car manufacturers often conceal dangerous vulnerabilities of their cars, and have found security glitches in the operation of these vehicles which allow hackers to control one or more vehicle aspects.

Over the last decade, cybercrime has continued to increase, impacting governments, corporations, and individuals.[15] Security researchers are the leading force in this country attempting to resolve these cybersecurity issues through diligent research and by actively circumventing these technologies to identify potential security vulnerabilities. What should be a primary concern in today's society is getting pushed to the wayside because manufacturers and copyright owners are threatening security researchers with copyright infringement suits for circumventing their software and technology. If the DMCA is going to remain the governing standard for the circumvention of software and technology, a permanent exemption for security researchers needs to be provided.

This article will provide an analysis of current cybersecurity issues and ways in which each can be resolved through reasonable and necessary good faith circumvention. It will also emphasize the need for permanent circumvention exemptions by the U.S. Copyright Office, and analyze whether the Library of Congress and U.S. Copyright Office should be the governing authorities for circumvention laws. The first part of this article will focus on cybersecurity, describing what it is, how prevalent it is in today's society, and how it is connected to the Digital Millennium Copyright Act. The second part will center on the U.S. Copyright Office and its authority over the DMCA, the anti-circumvention regulations of the DMCA, and how these regulations specifically influence and affect cybersecurity. The third part will focus on why this is such a critical area that needs to be reviewed and will weigh both the pros and cons of maintaining the DMCA's anti-circumvention exemption in favor of security research. Through a thorough review of the DMCA's effect on cybersecurity and research, the reader will gain insight into the influence the Library of Congress can have on security research and cybersecurity issues.

The existing literature focuses on ways research has been restricted, but is incomplete as to a more encompassing perspective. This article will focus on a broader view, discussing current literature that highlights the pros and cons of anti-circumvention under the DMCA, the influence the DMCA has on cybersecurity, and potential solutions to DMCA reform and governance. Indeed

[15] Laberis, Bill. "20 Eye-Opening Cybercrime Statistics." *Security Intelligence*, 14 Nov. 2016, securityintelligence.com/20-eye-opening-cybercrime-statistics/. (discussing cybercrime statistics and how they are continuing to evolve into a significant security issue for governments, corporations, and individuals alike).

some assert that the DMCA's anti-circumvention exemption could have prevented the Volkswagen scandal through a 1201 exemption for vehicles.[16] In contrast, the Environmental Protection Agency's argument against anti-circumvention exemptions (issued after the Volkswagen scandal) alleges the opposite.[17] This article will also discuss the comments the Electronic Frontier Foundation (EFF) submitted to the FDA surrounding the DMCA,[18] expanding upon the harsh side effects the anti-circumvention exemption has had on medical devices and the medical industry.

Moreover, the viewpoint of vehicle manufacturers and copyright owners should additionally be considered. This article will review various articles based on comments submitted to the U.S. Copyright Office and focus on the 1201 exemption, which provides perspective into why vehicle manufacturers are so keen on preventing software circumvention concerning tractors and vehicles. Also, this paper will discuss Senator Markey's report confronting the cyber-security issues surrounding anti-circumvention of vehicle software.[19]

Through an analysis of the DMCA anti-circumvention exemptions, how the exemptions have developed over the last ten years, and the case law surrounding both the positives and negatives of utilizing circumvention for research, this article will provide an awareness of progressive solutions for both researchers and copyright owners.

I. SECURITY RESEARCH IS ESSENTIAL FOR CYBERSECURITY DEVELOPMENT

This part will provide an overview as to what cybersecurity entails, why cybersecurity is essential for the United States, and how vital security research and an anti-circumvention exemption are for furthering cybercrime prevention. Further, this chapter will provide a descriptive analysis on how the anti-

---

[16] *See* Kit Walsh, *Researchers Could Have Uncovered Volkswagen's Emissions Cheat if Not Hindered by the DMCA*, Electronic Frontier Foundation. (Sept. 21, 2015).

[17] *See* The U.S. Copyright Office, *Environmental Protection Agency asks the US Copyright Office to Disregard Proposals in Favor of Anti-Circumvention Exemptions,* https://www.copyright.gov/1201/2015/USCO-letters/EPA_Letter_to_USCO_re_1201.pdf. (explaining why the EPA believes anti-circumvention exemptions should be amended or removed); Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 82 Fed. Reg. 29,804, 29,804-08 (June 30, 2017) (to be codified at 37 C.F.R pt. 201) (explaining why anti-circumvention exemptions should be amended or removed).

[18] *See* Electronic Frontier Foundation, *Postmarket Management of Cyber-security in Medical Devices,* https://www.eff.org/files/2016/04/22/electronic_frontier_foundation_comments_cybersecurity_in_medical_devices_.pdf.

[19] *See* Senator Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, http://www.markey.senate.gov/imo/media/doc/2015-02-06_markeyreport-tracking_hacking_carsecurity%202.pdf (last visited Sep 26, 2016).

circumvention exemption plays into security research.

A. What is Cybersecurity?

Cybersecurity issues embody much of the same elements as fundamental security issues. However, cybersecurity is still widely undervalued. According to the U.S. code, a cybersecurity incident is defined as a: "malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks." 16 U.S. Code § 824o(a)(8).[20]

So how do we translate this? Much like having bank robbers physically break into a bank to steal money by threat of violence or force, hackers can cause just as much damage by breaking into banks and accounts online, to take both money and personally identifiable information (PII). In broader terms, a cybersecurity incident can be anything from a hacker breaking into private email servers, to a hacker controlling the software for the brakes on an automobile,[21] both of which are serious security concerns the United States is currently facing.

The common misconception is that cyber-attacks happen to one in a million people. In 2015 alone, there was an average of 1.5 million cyber-attacks; in 2014, 47% of Americans had personally identifiable information stolen by hackers. In 2013, 43% of companies experienced data breaches which allowed hackers to steal company information.[22]

In total, over 594 million people are affected worldwide by cybercrime attacks every year.[23] Furthermore, analysts are now predicting the costs of cybercrimes to reach $2 trillion by 2019.[24] That is, cybercrime will amount to almost $500 billion

---

[20] 16 U.S.C. § 824o(a)(8) (2012). (Section 215 of the Federal Powers Act. Defines cyber-attack.).

[21] Jeff Kosseff, *The Cybersecurity Privilege,* 12 I/S: A J. of L. & Pol. for the info. Soc'y 261, 261 (2016) (defining types of cybersecurity incidents) (This article describes types of cybersecurity incidents, ranging from service attacks, data theft, website defacement, and other incidents).

[22] *See* CBS, CSI: Cyber, *These Cybercrime Statistics Will Make You Think Twice About Your Password: Where's the CSI Cyber team when you need them?* (2015), http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/. (discussing cybersecurity statistics and the number of times Americans have had personally identifiable information stolen throughout the last few years.).

[23] *See Norton Cybersecurity: Internet Security Threat Report* (2015) (Oct. 15, 2017), https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_p1_seeglobalrpt (Statistics on cybersecurity breaches as reported by Norton Software Company).

[24] *See* Steve Morgan, *Cyber Crime Costs Projected To Reach $2 Trillion by 2019*, FORBES, (2016), http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3e6642073bb0 (Cybersecurity cost predictions for the next few years, estimated based on current cybersecurity precautions in place.).

more than the debt the United States currently owes China.[25]

Cyber-attacks are a genuine and serious concern to the United States, and a robust cybersecurity program is essential to prevent, preclude, and mitigate attacks from occurring. Currently, the Department of Defense (DOD), the Department of Homeland Security (DHS), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are some of the main agencies that monitor, detect, and fight against cybercrime attacks. To prevent the furtherance of cyber-attacks, President Obama established the National Cybersecurity and Communications Integration Center in October of 2009 to serve as the nation's central hub for cybercrime prevention.[26]

Both the NSA and the DHS understand the importance and necessity of producing security researchers and experts in the field of cybercrime prevention. So in 2010, they created the *Centers of Academic Excellence in Information Assurance Education and Research* to facilitate programs that can directly produce experts in the field of cybercrime and cybersecurity research.[27] Furthermore, the DHS created an entire agenda and roadmap aimed at developing a progressive research and development plan to advance cybersecurity research.[28] These are just a few of the recent measures that have been taken to further security research in the promotion of cybercrime prevention.

B. How Cybersecurity Research Impacts Security Issues

Cybercrime attacks can target anyone and anything; this can consist of identity theft, controlling a vehicle, changing election votes, and breaking into email accounts. Security research can prevent the growing number of cybercrime

---

[25] Becket Adams, *Chart: Who Does the U.S. Gov't Owe $17 Trillion To?* THEBLAZE, (Oct. 15, 2017) http://www.theblaze.com/stories/2013/10/12/chart-who-does-the-u-s-govt-owe-17-trillion-to/ (Web story detailing the amount of money the United States owes China – used to emphasize how much cybercrime attacks can cost the United States).

[26] *See* Office of the Press Secretary, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center New National Cybersecurity Center Opened* HOMELAND SECURITY, (Oct. 15, 2017) https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened (President Obama's plan for preventing cyber-attacks through the implementation of additional cybersecurity centers focused on cybercrime prevention and security research).

[27] *See* Department of Homeland Security's Library, *Preventing and Defending Against Cyber Attacks,* (Sept. 2010), https://www.dhs.gov/xlibrary/assets/defending-against-cyber-attacks-september-2010.pdf (Along with President Obama's administration, the DHS and NSA have created cybersecurity-focused centers that work on security research as a principle method to prevent future cyber-attacks).

[28] *See* Department of Homeland Security Cybersecurity, *A Roadmap for Cybersecurity Research,* (Nov. 2009), https://www.dhs.gov/sites/default/files/publications/csd-dhs-cybersecurity-roadmap_0.pdf.

attacks that occur hourly and can develop mitigation strategies to stop, isolate, and prevent recurrences.[29]

As mentioned above, government agencies are continuously establishing programs which advance the United States' knowledge and research in cybersecurity. In sum, cybersecurity research can grant experts and researchers the ability to develop solutions that can prevent hackers from attacking companies, the government, and citizens. While cyber-attacks were formerly centered on email or credit card hacks, cybercrime attacks have evolved with the digital age, and allow hackers to cast a wider net over the digital devices consumers use on a regular basis.

Recent cybercrimes reported in the news focus on attacks on medical implants and vehicle software. Cybersecurity researchers have found deadly vulnerabilities in a variety of medical devices, including pacemakers and insulin pumps. These vulnerabilities grant hackers the opportunity to access and control these implants through hacking the medical system software.[30] This means that anyone who relies on a medical implant to sustain their life, such as a pacemaker, could face death if a hacker targeted the security vulnerabilities in the device and switched the device off.

Vehicle software has also been a recent target of hackers. Researchers who have been able to circumvent vehicle software have found security issues that could have a dangerous impact on consumers who drive cars.[31] Through circumventing vehicle software, researchers have detected a few ways in which hackers have been able to control vehicles,[32] such as, controlling the brakes and the steering in a vehicle by gaining access through the vehicle's Bluetooth or other communication ports. The recent recall by Fiat is one instance in which a security researcher's circumvention of vehicle software potentially saved lives. Security researchers found the security vulnerability when circumventing the vehicle; these researchers were able to show Fiat just how easily they could control the vehicle and brakes through a communication port on the vehicle. As a

---

[29] Kayla Morency, *Cybersecurity Finally Takes Center Stage In The U.S.*, 15 J. HIGH TECH. L. 192 (2014) (focuses on various areas of cybersecurity research and how this research can minimize cybersecurity threats).

[30] Robert A. McFarlane & Timothy v. Fisher, *Software Patents Under 35 U.S.C. § 271(f): Should Congress Amend § 271 to Harmonize Protection Between Tangible and Intangible Inventions?*, 2 HASTINGS SCI. & TECH. L.J. 183 (2010) (discussing major cases covering pacemakers and circumvention exemptions for this type of software).

[31] Antigone Peyton, *The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World*, 24 CATH. U. J. L. & TECH. 36 (2016).

[32] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944 (the most recent version of circumvention exemptions for automobiles).

result, Fiat recalled 1.4 million of their vehicles.[33]

An anti-circumvention exemption for security research is essential in preventing dangerous hacks. Cybersecurity research has already proven to be effective in preventing future cybercrimes and should remain a priority for the United States; however, security researchers have hit snags due to threats of copyright infringement by software manufacturers who feel that circumvention is a form of copyright infringement. These software owners and manufacturers have implemented specific access-control measures in their works to prevent users from accessing the work, and these are the barriers researchers are circumventing. Circumvention is essentially the method by which a person breaks into a device's software, bypassing technological protection measures that control access to the device.[34] As defined, circumvention means: "To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[35]

In the past, circumvention was most commonly associated with hackers pirating music or movies; however, more recently circumvention has been widely publicized in relation to security researchers. Security researchers have been circumventing various types of software, to detect security flaws and vulnerabilities in the device's system. These acts of circumvention are the reason why many manufacturers and digital copyright owners have been lobbying the Library of Congress to remove the anti-circumvention exemptions under the Digital Millennium Copyright Act;[36] however, removing the anti-circumvention exemption would have a negative impact on security research.

To continue developing advancements in cybersecurity, security research will likely need to maintain a permanent anti-circumvention exemption. The Library of Congress and the U.S. Copyright Office are the governing authorities over the DMCA and are the sole authorities to implement and amend exemptions.[37] In effect, if the Library of Congress and the U.S. Copyright Office make the current anti-circumvention exemptions permanent, then security researchers will be able to circumvent software and technology to detect security vulnerabilities and find

---

[33] *See Peek into the Future: The Risk of Things*, Symantec, https://www.symantec.com/content/dam/symantec/docs/infographics/istr-iot-en.pdf. (detailing Fiat's recent recall due to the discovery of hackable software by security researchers located in some of Fiat's vehicles).

[34] 17 U.S.C. § 1201(a)(1) (defining technological protection measures).

[35] *Id.* (defining circumvention regarding TPM's in software relating to copyright infringement violations).

[36] *Id.* at §1201(a)(1)(A) (no individual is authorized to circumvent TPM's, put in place to prevent copyright infringement).

[37] June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385 (2004).

adequate solutions to prevent potentially deadly hacks and do so without fear of prosecution.

II. INCOMPLETE PROTECTIONS IN THE DMCA

This part will focus on the history, evolution, and responsibilities maintained by the Library of Congress and the U.S. Copyright Office; the evolvement of the Digital Millennium Copyright Act and its exemptions; and how the two affect cybersecurity.

A. History Behind the Library of Congress and U.S. Copyright Office

Copyright law was created to protect original works of authorships.[38] One way it extends to digital media is through the Digital Millennium Copyright Act.[39] Beginning in the 1800s, the Library of Congress was the sole agency that handled copyrighted works and registries. Over time, the Library of Congress expanded, adding the U.S. Copyright Office as a branch of the Library of Congress. Today, the U.S. Copyright Office operates by working with copyright owners who are in the process of registering their works, while also reviewing former registered works.[40] Essentially, the U.S. Copyright Office serves as a place of copyright records, where claims of registered copyrights are kept and are searchable for owners interested in registering their copyrights.[41] The U.S. Copyright Office has remained a branch of the Library of Congress and, when requested, provides advice to Congress surrounding the creation and enforcement of copyright laws.[42]

Every three years, the U.S. Copyright Office reviews comments and policy proposals from scholars, authors, and other individuals, seeking specific changes in copyright laws and legislation.[43] More recently, these comments focus on the anti-circumvention exemptions under Section 1201 of the DMCA. As noted earlier, the U.S. Copyright Office provides Congress with suggestions surrounding copyright law changes and Congress makes the final determination on what laws to amend. When advising Congress on copyright law changes, the

---

[38] Copyright Act of 1976, 17 U.S.C. § 102 (2012) (protecting original works of authorships that are fixed in a tangible medium. These forms of copyright can be anything from books and motion pictures, to software).

[39] 17 U.S.C. § 1201 (2012).

[40] *See* U.S. Copyright Office, *Policy Reports,* https://www.copyright.gov/policy/policy-reports.html (the US Copyright Office uses proposed comments they have received from third parties to help create copyright legislation surrounding the DMCA including the circumvention of TPMs).

[41] *See* U.S. Copyright Office, *Overview of the Copyright Office* (December 2016) https://www.copyright.gov/about/ (last visited Dec. 1, 2016).

[42] *See id.*

[43] *Id.* at §1201(g)(1)(c).

U.S. Copyright Office references proposals and comments received from scholars, agencies, and corporations.[44]

Two laws govern copyright matters before the Library of Congress and the U.S. Copyright Office: the Copyright Act of 1976 and the Digital Millennium Copyright Act.[45] The Copyright Act of 1976 dictates many issues relating to copyright law and sets out the rights copyright owners retain.[46] The DMCA was enacted to target copyright issues relating to digital services and content.

B. The DMCA and the 1201 Exemption

With the continuing evolution of the digital age, the U.S. Copyright Office has gravitated from its original purpose of registering copyrights and serving as a copyright records office, to regulating copyright and copyright use through the implementation of laws, such as the DMCA.[47] The DMCA was created to provide a more in-depth digital media and technology focused set of copyright laws, and to outline penalties for unauthorized uses and infringement.

The DMCA consists of multiple exemptions, ranging from Fair Use exemptions to the recently added temporary anti-circumvention exemptions for security researchers over vehicle software and medical implants.[48] This exemption could become permanent, but for now it maintains a three-year time limit and will allow a security researcher to circumvent technology software, so long as the circumvention qualifies as 'good faith security research.' The new rule defines "good-faith security research" as:

> accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability... and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates ... and is not used or maintained in a manner that facilitates copyright infringement.[49]

---

[44] *See Policy Reports*, U.S. COPYRIGHT OFFICE, https://www.copyright.gov/policy/policy-reports.html (proposing comments they have received from third parties to help create copyright legislation surrounding the DMCA, including the circumvention of TPMs).

[45] *See Overview of the Copyright Office,* U.S. COPYRIGHT OFFICE, https://www.copyright.gov/about/.

[46] Copyright Act of 1976, Pub. L. No. 94 - 553, 90 Stat. 2541 (1976).

[47] 17 USC § 1201.

[48] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R § 201(2014) (discussing the DMCA's exemptions surrounding anti-circumvention by security researchers).

[49] *See* Charlie Osborne, *US DMCA rules updated to give security experts legal backing to research*, Zero Day (2016), http://www.zdnet.com/article/us-dmca-rules-updated-to-give-security-experts-legal-backing-to-research/ (discussing the updated anti-circumvention exemption

This new amendment to the DMCA serves as a positive step for furthering cybercrime prevention through security research and allows researchers the opportunity to discover security vulnerabilities through the circumvention of targeted software. This amended exemption also extends to the circumvention of some consumer and household items, including medical implants, electric toothbrushes, vehicles, smart TVs, and more.[50]

Before the amended 2015 exemption, there was an existing exemption for security research under 1201(g); however, many researchers have found the exemption to be overbearing due to the exemption's requirement of obtaining permission from the software owner. More specifically, this DMCA 1201(g) exemption for security research requires the researcher to show that the published work was lawfully obtained, a good faith effort was used to obtain authorization before circumventing the work, and that the act does not constitute an infringement. [51]

Under 1201(g), if the researcher does not meet all the requirements of the exemption and a lawsuit results, the court will balance the interest of all parties when deciding if the circumvention threat constitutes copyright infringement.[52] When deciding if the act constitutes copyright infringement, the court balances "the needs of law enforcement and other government agencies, computer programmers, encryption researchers, and computer security specialists' against the issue of circumventing software." [53]

As technology and digital advancements continue to develop, the DMCA exemptions will need to advance as well, evolving with the technology and innovations. This need to advance is one of the central reasons the U.S. Copyright Office and the Library of Congress continue to amend and remove particular exemptions requiring updates.

---

pertaining to security researchers circumventing software and TPM's for good faith security research)(discussing the *DMCA security research exemption for consumer devices,* Federal Trade Commission, https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices).

[50] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944 (Oct. 28, 2015) (stating the several types of software that may now be circumvented for security research purposes under the anti-circumvention exemptions).

[51] *See* 17 U.S.C.S. § 1201(g)(2).

[52] *Id.*

[53] *See* United States v. ELCOM Ltd., 203 F. Supp. 2d 1111, 1130–31 (N.D. Cal. 2002) (discussing the need for an anti-circumvention exemption for security purposes. The Court balances the interest of each party involved in a suit to determine if a circumvention threat is present. Ultimately, balancing the infringement implications against potential security threats).

C. The DMCA's Restriction on Security Research

For the last decade, the DMCA has placed a substantial burden on security researchers who have been working to prevent cybersecurity issues. Although the DMCA anti-circumvention exemptions have recently been modified and tend to create a less restrictive exemption, there remains speculation as to whether the exemption will be effective as a temporary exemption, or whether a more permanent law is necessary.[54] Many organizations and scholars have submitted comments and proposals to the U.S. Copyright Office, thereby expressing their desires for the temporary exemption to become a permanent exemption.

Before the addition of the 2015 temporary anti-circumvention exemption, many issues could have been avoided if the exemption for security research circumvention existed. In 2015, Volkswagen attempted to mask vehicle emissions information through alterations the manufacturer made in the vehicle's software.[55] This demonstrates how the emission scandal could have been detected if there had been an anti-circumvention exemption in effect.[56] Specifically, security researchers would have been able to circumvent the Volkswagen vehicle software to discover the emission issues before these Volkswagen vehicles were distributed on the market.[57]

The Electronic Frontier Foundation (EFF), a non-profit organization that primarily works to defend civil liberties in the digital world,[58] submitted comments and proposals to the U.S. Copyright Office based on the security issues involved with the Volkswagen case and sought an amendment of the anti-circumvention exemptions and maintained that if an anti-circumvention exemption for vehicle software had existed in the DMCA before this incident, Volkswagen would not have been able to conceal their faulty vehicle emissions.[59]

---

[54] *See* Charlie Osborne, *US DMCA rules updated to give security experts legal backing to research, Zero Day* (2016), http://www.zdnet.com/article/us-dmca-rules-updated-to-give-security-experts-legal-backing-to-research/.

[55] Kit Walsh, *Researchers Could Have Uncovered Volkswagen's Emissions Cheat if Not Hindered by the DMCA*, Electronic Frontier Foundation. (Sept. 21, 2015) (examining and evaluating how security research through circumvention could have prevented the Volkswagen emissions scandal).

[56] *See id.*

[57] *See* Blake Brittain, *DMCA at Issue After Volkswagen Emissions Scandal*, Bloomberg BNA (Oct. 6, 2016), http://www.bna.com/dmca-issue-volkswagen-n57982058743/ (discussing the outcome of the Volkswagen case if there had been an exemption for vehicle software circumvention, under the DMCA, researchers would have been able to discover the issue much sooner).

[58] *See about EFF, Electronic Frontier Foundation* (2014) https://www.eff.org/about (explaining who the EFF is and their organization's mission).

[59] *See* Blake Brittain, *DMCA at Issue After Volkswagen Emissions Scandal*, BLOOMBERG BNA (Oct. 6, 2016), http://www.bna.com/dmca-issue-volkswagen-n57982058743/.

Further, they found it entirely reasonable that a security researcher would have been able to detect the emission violations before the vehicles were placed in the stream of commerce, and therefore could have prevented the issues that resulted due to Volkswagen's concealment. [60]

The EFF also submitted a comment and proposal to the Food and Drug Administration (FDA), requesting the FDA to implement a policy to protect security researchers from lawsuits relating to medical devices. The EFF asked the FDA to maintain a policy whereby a vendor could only obtain approval for their medical implant if they agreed to not bring any suits under the DMCA and against security researchers. In exact terms, the EFF requested that the FDA "require that vendors covenant, as a condition of approval of their devices for field use, to abstain from the use of DMCA 1201 for causes of action related to security research."[61]

Another incident that reiterated the need for security research and circumvention exemptions surrounding vehicle software was the Chrysler recall. In 2015, Chrysler had to recall over one million vehicles due to a security vulnerability discovered by security researchers to be a "hackable issue" located in Chrysler's dashboard computers.[62] This type of hack is extremely hazardous, as it can enable a hacker to obtain control of the steering, transmission, and brakes of another person's vehicle by hacking the vehicle software.[63] If the security researchers who discovered the vulnerability in the software would have been able to circumvent the software before the vehicles were sold, then Chrysler would not have had to initiate the recall, and arguably, the potential vulnerability may have been mitigated before such vehicles entered the marketplace.

Although hacking a vehicle's software to control the functionality and steering of the car is the most dangerous form of vehicle cyber-attack to date, it is not the only area of security concern surrounding vehicles. In the United Kingdom, there are car theft cases based on hackers breaking into the keyless entry system.[64]

---

[60] Kit Walsh, *Researchers Could Have Uncovered Volkswagen's Emissions Cheat if Not Hindered by the DMCA*, Electronic Frontier Foundation (Sept. 21, 2015).

[61] *See Postmarket Management of Cyber-security in Medical Devices*, Electronic Frontier Foundation (April 21, 2016), https://www.eff.org/files/2016/04/22/electronic_frontier_foundation_comments_cybersecurity_in_medical_devices_.pdf (asking the FDA to mandate a policy where every medical manufacturer, as a condition to receiving certification from the FDA, promise not to utilize the DMCA in regards to security research).

[62] Jenna Genio, *New US Rule Allows Ethical Hacking into Cars,* AUTO INDUSTRY NEWS (Nov. 11, 2016), https://www.autoindustriya.com/auto-industry-news/new-us-rule-allows-ethical-hacking-into-cars.html.

[63] *See id.*

[64] *See Peek into the Future: The Risk of Things*, Symantec (last visited November 8, 2016), https://www.symantec.com/content/dam/symantec/docs/infographics/istr-iot-en.pdf.

More specifically, hackers were breaking into the vehicle's digital keyless system and vehicle software and unlocking the car to steal the vehicle. This is another scenario which could have been prevented if security researchers had been allowed to circumvent the software in advance to detect security flaws. Some vehicle manufacturers, including Tesla, are now offering monetary awards to white hat hackers who discover any issues or bugs in their automotive software.[65] The only condition is that the issues must be disclosed to the company discreetly.[66]

Currently, the United States has close to 6.4 billion internet-connected devices, ranging from watches, cellphones, vehicles, TVs, and GPS devices.[67] Symantec, a technology corporation that produces software for security purposes, predicts the United States will have over 20.8 billion internet-connected products before the year 2020.[68]

D. Opposition to Anti Circumvention Exemptions

Although amending the anti-circumvention exemption provides security researchers with a better platform to prevent cybercrimes, many copyright owners and agencies have raised questions as to if this exemption violates copyright law, and if it also has the potential to cause unforeseen injury through misuse and abuse.[69]

John Deere, a tractor manufacturing company, submitted comments to the U.S. Copyright Office requesting the removal of anti-circumvention exemptions.[70] John Deere argued in their comments that there should be no exemption allowing vehicle circumvention because it was a form of copyright infringement since technically John Deere still owns the programming located in each John Deere tractor sold. The submitted comment elaborates on how John Deere's ownership of the programming entitles Deere to be the only entity with rights to access the software and that even the tractor owner has no rights to

---

[65] *See* Genio, *supra* note 62.
[66] *See id.*
[67] *See* Brittain, *supra* note 59.
[68] *See id.*
[69] Thomas A. Mitchell, *Copyright, Congress, and Constitutionality: How the Digital Millenium Copyright Act Goes Too Far*, 79 NOTRE DAME L. REV. 2115, 2115 (2004) (discussing the DMCA and the ways it oversteps and endangers the rights of consumers and prevents circumvention).
[70] Darin Bartholomew, John Deere & Co., *Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, U.S. Copyright Office (Mar. 3, 2016) ("in the absence of TPMs third-party software developers could purchase vehicles to access instantly copyrighted, safe and regulatory-compliant software that is the result of years of extensive research and development by manufacturers and suppliers."); *The Internet of Things: Where Privacy and Copyright Collide*, 33 SANTA CLARA HIGH TECH. L.J. 90, 101 (2016).

access the software. Further, John Deere goes on to state that allowing the owners of these tractors to circumvent the tractor's software could cause further issues because giving third parties access permits software infringement.[71] Although John Deere's argument appears unfounded, it does raise an important issue if this circumvention qualifies as a form of copyright infringement.[72]

The Environmental Protection Agency (EPA) brought a different argument to the U.S. Copyright Office, focusing its proposal on the harm the exemption could do to the environment through emission tampering in [motor] vehicles, and that these exemptions would 'hinder their ability to enforce tampering prohibitions.[73] "Under section 203(a), the Agency has taken enforcement action against third-party vendors who sell or install equipment that can "bypass, defeat, or render inoperative" software designed to enable vehicles to comply with CFAA regulations. EPA can curb this practice more effectively if circumventing TPMs remains prohibited under the DMCA."[74]

The EPA further asserts the anti-circumvention exemptions are not needed since car manufacturers run their own diagnostics and do not require security researchers to help them detect vehicle vulnerabilities.[75] Further, the EPA noted that even if the barriers and TPMs contained in vehicle software were not intended to preclude researcher access, such restrictions are still relevant because each can possibly prevent unlawful tampering of the software by unauthorized users.[76]

Additionally, scholars have expressed discontent for the anti-circumvention exemptions as being pointless; arguing that hackers who are illegally circumventing software will continue to do so whether or not there is a law in effect prohibiting such access, and therefore the law has no significant impact.[77] Although these scholars are not in favor of the anti-circumvention exemptions, they do support circumvention for security research. These scholars acknowledge the intent behind the creation of the anti-circumvention exemption; however,

---

[71] *Id.*

[72] *See Long Comment Regarding Proposed Exemption Under 17 U.S.C. 1201*, U.S. Copyright Office, http://copyright.gov/1201/2015/comments-032715/class. 21/john_deere_class21_1201_2014.pdf (last visited Oct. 26, 2017) (discussing the anti-circumvention exemptions of the Copyright Office, and why they should be removed due to copyright infringement violations).

[73] *See* Environmental Protection Agency asks the US Copyright Office to Disregard Proposals in Favor of Anti-Circumvention Exemptions, U.S. Copyright Office (July 17, 2015), https://copyright.gov/1201/2015/USCO-letters/EPA_Letter_to_USCO_re_1201.pdf.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] Tian, YiJun. "Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions." *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 15, no. 3, 2005, pp. 767–772.

these laws only act as a barrier against those who wish to circumvent the software in good faith, as hackers will break the law regardless of the exemption.[78] Therefore, if the anti-circumvention exemptions are only preventing the good faith users from circumventing software, it raises the question of whether circumvention laws should even exist.

Instead of submitting comments to the U.S. Copyright Office, Senator Markey took a different approach and contacted the most prominent vehicle manufacturers about vehicle security concerns and safeguards each has implemented since the vehicle security hacks.[79] This information was provided in Senator Markey's report detailing vehicle security vulnerabilities.[80] The report provides details on ways the vehicles have been modified, including new digital safety features; however, these new digital safety features remain pieces of accessible technology and therefore are just as likely to be accessed and controlled by hackers as before the modifications.[81] The report also specified that vehicle safety concerns were often by the vehicle manufacturer, but with the incidences that arose out of Volkswagen, Jeep, and Chrysler, much uncertainty remains as to the security of any vehicle software that has not been tested by security researchers. Senator Markey's report also highlights the significant cyber-attacks that have occurred in vehicle software, and why there needs to be more security research in testing vehicle software systems, stating:[82]

> There are no assurances that these vehicles are the only ones that are this unprotected from cyber-attack. A safe and fully-equipped vehicle should be one that is equipped to protect drivers from hackers and thieves. Both automakers and NHTSA should be immediately taking steps to verify that other similar vulnerabilities do not exist in other models that are on the road.[83]

Cybersecurity research exemptions are difficult to get passed in the United States, and the DMCA is not the only set of laws facing difficulty with security research exemptions. The Electronic Communications Privacy Act (ECPA) is a

---

[78] *See* David Nimmer, Nimmer on Copyright Volume 11 Appendix 62 (Matthew Bender ed. 2017).

[79] *See generally Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, http://www.markey.senate.gov/imo/media/doc/2015-02-06_markeyreport-tracking_hacking_carsecurity%202.pdf (last visited Nov. 21, 2017) (discussing new car technologies that leave room for hackers to gain control of essential car functions and protections against hacking).

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *See* David Shepardson, *Fiat Chrysler Will Recall Vehicles over Hacking Worries,* THE DETROIT NEWS (July 24, 2015), http://www.detroitnews.com/story/business/autos/2015/07/24/us-pushing-guard-vehicle-cyberhacking/30613567/.

set of laws that govern communication privacy and can relate to emails, internet browsing history, online instant messaging conversations, and other similar forms of electronic communication.[84] Like the DMCA, the ECPA needs a cybersecurity research exemption; however, it is not favored because much of the general public has expressed disapproval in granting access to personal emails and web history to security researchers.[85] Unlike the ECPA, the DMCA does have a temporary anti-circumvention exemption, and it contains an encryption research exception,[86] although many scholars have criticized the exemption as being too narrow to be of practical use.[87]

III. REFORM SOLUTIONS FOR SECURITY RESEARCH

With a grasp on the concepts of cybersecurity and security research; the DMCA, its anti-circumvention exemptions and its effect on cybersecurity; and how the U.S. Copyright Office and Library of Congress govern the DMCA – an examination of reform solutions for anti-circumvention exemptions follows.

A. Amending the Anti-Circumvention Exemptions

One of the commonly proposed Section 1201 reform solutions remains to create a permanent anti-circumvention exemption that will continue to allow security researchers to more freely find solutions to security vulnerabilities through circumvention. The current anti-circumvention exemptions have been received as a positive step forward by much of the academic and security community; however, this exemption is only set for three years and then has the potential to be amended.[88] The DMCA needs to maintain a permanent exemption that will grant the circumvention of software and technology for good faith security research purposes, equating to a stronger balance in favor of the public good.

As shown in the Volkswagen and Chrysler cases, security research has already proven to be significantly helpful in detecting security issues and vulnerabilities.[89] Security researchers need to be able to continue circumventing software and

---

[84] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

[85] *See generally* Aaron Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 168, 197 (2008) (discussing a recent study of consumer beliefs).

[86] *See* 17 U.S.C. § 1201(g) (2012).

[87] *See* Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501, 509 (2003) (discussing the DMCA's regulation of scientific research versus other laws that are still having difficulty with security research exemptions).

[88] *See* Charlie Osborne, *US DMCA rules updated to give security experts legal backing to research*, ZDNET (Oct. 31, 2016, 3:56 PM), http://www.zdnet.com/article/us-dmca-rules-updated-to-give-security-experts-legal-backing-to-research/.

[89] *See* Genio, *supra* note 62.

technology to detect and prevent cyber issues. The Energy and Commerce Committee Chairman, Fred Upton, also vocalized the necessity of evolving policy with the evolving technology:

> Innovation is occurring at lightning speed, and the intersection of automobiles and technology offers tremendous opportunity to keep families safe on the road and improve the American driving experience. But as the underlying technologies seemingly evolve by the day, so too must our manufacturers and regulators keep pace to protect drivers from these growing threats.[90]

So what solutions are there for maintaining anti-circumvention exemptions or laws? Some scholars have recommended using the DMCA's Fair Use exemption to act as a mold for creating a permanent anti-circumvention exemption – "Fair Circumvention."[91] Using the same elements that are used for Fair Use, but matching the elements with circumvention, could serve as a way to maintain a permanent circumvention exemption while still taking into account any infringement uses and issues that may arise. As discussed in some law articles, the DMCA is unclear as to what is covered under the anti-circumvention exemption that courts have been using as a case by case approach with uncertainty over what the circumvention exemption entails.[92] If the U.S. Copyright Office modifies the anti-circumvention exemption under the DMCA while mirroring the Fair Use elements, this exemption has the potential to create a fair balance between the copyright owners and good faith researchers and also balance the public good against the rights of intellectual ownership.

Another proposed solution for the anti-circumvention exemption would be to amend the wording of the provision. Many experts in the field of technology and circumvention disfavor the current DMCA anti-circumvention exemption due to its vagueness, and they attribute this factor as being one of the reasons content producers are over-copyrighting their works to prevent access to their technology and software.[93] After reviewing the *MGE UPS Systems* case,[94] it becomes even more apparent that there is a substantial need for clarification and rephrasing of

---

[90] David Shepardson, *Fiat Chrysler Will Recall Vehicles over Hacking Worries,* THE DETROIT NEWS (July 24, 2015), http://www.detroitnews.com/story/business/autos/2015/07/24/us-pushing-guard-vehicle-cyberhacking/30613567/.

[91] *See* Timothy K. Armstrong, *Fair Circumvention*, 74 BROOKLYN L. REV. 1, 4 (2008).

[92] *Id.* at 3.

[93] *See* James L. Davis, Note, *Is Interoperability Just for Those Who Can Hack It? The Application of the DMCA Interoperability Exceptions in the Consumer Electronics Industry*, 2005 U. ILL. J.L. TECH. & POL'Y 141-43 (2005) (discussing product manufacturers' use of microchips, which require an authorization sequence, as an anti-competitive method to prevent other product manufacturers from selling replacement or compatible products).

[94] *See, e.g.*, MGE UPS Sys. v. Gen. Elec. Co., 622 F.3d 361 (5th Cir. 2010); Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1195 (Fed. Cir. 2004).

the DMCA. These cases were initially decided by balancing the interests of both the copyright owners and the users. This balancing test led to a misinterpretation of the laws in the DMCA and what the DMCA covered. Originally the court misconstrued the meaning of 'access' in the DMCA and thought it meant access that gives rise to the protections under copyright law, but in reality, it was simply meant as "access" to a software or product.[95]

When considering solutions for the anti-circumvention exemption, it has been suggested that the U.S. Copyright Office and Library of Congress review the European Union's approach to circumvention. Compared to the DMCA, the EU regulations are more lenient and allow experts to circumvent software and products on behalf of another who has ownership rights in the product.[96] The U.S. Copyright Office could make a provision like this, allowing security researchers to circumvent software for good faith security purposes with a caveat that each must share the vulnerabilities discovered with the copyright owner – quid pro quo. This would grant security researchers more opportunities to discover security vulnerabilities, and possibly prevent cyber-attacks.

B. Should the U.S. Copyright Office Oversee the DMCA?

In years past, the U.S. Copyright Office has moved from registering copyrights to regulating copyright law, as seen with the DMCA. There is an ongoing debate if the Library of Congress and the U.S. Copyright Office have the requisite expert knowledge to create laws governing anti-circumvention and technology. One proposed Section 1201 reform solution is to shift the governing authority over the DMCA to another agency or organization that consists of experts in the digital field. Scholars have suggested that allowing experts in this field to govern the DMCA, instead of the Library of Congress, would be more beneficial to both the software owners and the users. Although the Library of Congress is a neutral party, this entity is not an expert in the field; therefore, it does not have the requisite knowledge over the intricacies involved in software circumvention.[97]

Additionally, the public interest concern should be reviewed. General Motors

---

[95] *See* Noah J. Wald, *Don't Circumvent my Dongle! Misinterpretation of the Digital Millennium Copyright Act Threatens Digital Security Technology*, 33 T. JEFFERSON L. REV. 325, 342-358 (2011) (discussing the Fifth Circuit's misinterpretation of "access" in the *MGE UPS* case).

[96] *See id.*

[97] Feedback received from Jason Hong, an Associate Professor at School of Computer Science: Carnegie Mellon University. The DMCA needs to have input from experts in the field. Although the Library of Congress is a neutral party, they are not experts in the field. The exemptions also need to cover more areas for good faith security research (e.g., academics or white hat security researchers).

and other vehicle manufacturers have made compelling points in arguing that the DMCA helps prevent people from making dangerous hacks to their cars, where such modifications have the potential to cause injury to other people.[98] Nevertheless, the Library of Congress and U.S. Copyright Office should also consider the public interest when implementing laws that affect vehicle systems, as these laws have the potential to protect the public by allowing more security research through circumvention and testing. Vehicle software is extremely critical in managing and controlling vehicle operation; therefore, seeking to ensure that the vehicle software and systems have no vulnerabilities is essential for a driver, occupant, and in effect, public safety. The Library of Congress' amendment to the anti-circumvention exemption for vehicle software was in favor of public interest because it allowed security researchers to circumvent software for good faith security purposes to detect security issues and vulnerabilities. Although the newest anti-circumvention exemption provides circumvention for security research, a permanent exemption or solution needs to be mandated.

There are a variety of security agencies that focus on cybersecurity issues and ways to protect the United States from cybercrime attacks. A potential solution would be for Congress to delegate one of these agencies with authority to oversee the DMCA. Alternatively, Congress could create a committee made up of digital and cyber experts to regulate and govern the DMCA.

Another basis for removing the DMCA from the governing authority of the U.S. Copyright Office and Library of Congress is that the DMCA's purpose does not focus on copyright, but instead applies to works that are protected under copyright. To be protected under the DMCA and make use of the laws covered under the DMCA, a product must be copyrighted – therefore the copyright is only acting as a gate to utilize the DMCA. The DMCA itself is not copyright law. As one scholar put it, 'copyright is a property based model' whereas the 'DMCA controls access to the copyrighted property and prohibits circumvention of the copyrighted works.'[99] Additionally, the laws governing causes of actions and remedies differ from claims brought under copyright actions. When the DMCA is violated, the claim brought does not have to meet the requirements under copyright law. These laws further empower the laws of copyright by implementing a set of civil and criminal causes of action within the DMCA;[100] therefore, removing the DMCA from the authority of the U.S. Copyright Office and the Library of Congress would be one reasonable approach. Additionally, the DMCA could be designated to its own specific jurisdiction, similar to the model

[98] *See* Genio, *supra* note 62.

[99] *See* Arielle Singh, *Agency Regulation in Copyright Law: Rulemaking Under the DMCA and Its Broader Implications*, 26 BERKELEY TECH. L.J. 527-28 (2011).

[100] *See* 17 USC § §1203-1204 (2012).

that was constructed for Patents in the Federal Circuit Courts.[101] Designating the DMCA to its own jurisdiction would guarantee that the court hearing DMCA cases would have the knowledge necessary to rule on DMCA laws and would understand the technical verbiage in those laws. This approach could ensure that the court hearing DMCA cases will have the requisite knowledge to decide these cases; however, it does not provide a solution for security research and circumvention.

Another argument against the DMCA being governed by the Library of Congress and the U.S. Copyright Office is that it violates Article 1, but this is a weak argument. The U.S. Copyright Office is a subsidiary of the Library of Congress, making it an Article 1 agency. The issue arises under the U.S. Copyright Office's notice and comment procedure since it violates Article 1 law making requirements. When the DMCA was created, the U.S. Copyright Office was to act as "an executive branch entity",[102] but as the Copyright Office has continued to influence legislative rules, there has been no separation of power between its legislative and executive purpose.[103]

Another solution for governing the DMCA would be to expand the power of the U.S. Copyright Office and to place the DMCA solely under its authority. The U.S. Copyright Office often deals with digital copyrighted works and could maintain a division that individually handles technology, software, and digital copyrighted works. This would allow the U.S. Copyright Office to have sole authority over modifications of the DMCA; therefore, the DMCA could be governed by the division of technology experts that understand the complexities in technology and digital copyrighted works. However, if the power of the U.S. Copyright Office expanded and it became an executive branch agency under the President, this would present the danger of it becoming susceptible to private interest groups and parties.[104]

CONCLUSION: TOWARD THE FUTURE

Although there has been substantial growth and development in the DMCA's 1201 anti-circumvention exemptions, it remains unclear as to what will happen in another three years as the laws change again. As technology and the digital age continue to evolve, the laws that surround these new devices will also need to

---

[101] *See* Wald, *supra* note 95, at 358.

[102] *See* Andy Gass, *Considering Copyright Rulemaking: the Constitutional Question*, 27 BERKELEY TECH. L.J. 1047, 1058 (2012) (quoting President Clinton in the Presidential Statement on Signing the Digital Millennium Copyright Act, 34 Weekly Comp. Pres. Doc. 2168, 2169 (Oct. 28, 1998)).

[103] *See* Singh, *supra* note 86, at 531-32.

[104] *See id.* (Congress originally intended the DMCA to prevent piracy of DVDs, not software testing).

develop.

Cybersecurity is a crucial, and global necessity. Steps should be taken to expand its protective reach. Security research is one of those essential steps. Security research has already proven to be substantially useful in preventing cyber-attacks, and laws need to be maintained to continue its expanding footprint of strength, growth, and resiliency to meet the needs of an expanding cyber culture. With the creation of a permanent anti-circumvention exemption or a new law altogether, focusing on technology and circumvention, security researchers will have the ability to continue to find security glitches, flaws, and vulnerabilities to possibly prevent cyber-attacks and potentially save lives.

Alternatively, placing the DMCA under another agency also remains a viable solution. The National Security Agency, the Department of Homeland Security, and the Federal Bureau of Investigation all have divisions that focus on cybersecurity and preventing cyber-attacks. This technological knowledge of software and cyber warfare could be incredibly insightful in providing appropriate laws under the DMCA. Moving the DMCA to the sole authority of the U.S. Copyright Office is another potential solution. The U.S. Copyright Office understands the copyright laws and could maintain a division for digital copyrighted works, specifically tailored by industry experts who understand the technology and digital works complexities.

As technology and innovation continue to evolve, it is imperative that the laws governing technology evolve as well.

***