Reforming the Digital Millennium Copyright Act

Introduction

The Digital Millennium Copyright Act (DMCA) is a 1998 law which controls access to copyrighted digital works. In the last two decades, it has helped prevent copyright infringement by incurring penalties on those who illegally copy and modify protected works. However, the DMCA has had some unforeseen consequences, and as a result, the DMCA is used by software companies to inhibit independent security research into their proprietary software products. This jeopardizes the data security of customers, and plays an important role in the atmosphere of cyber insecurity illustrated by Bruce Schneier in *Click Here to Kill Everybody*. While the application of copyright to software is an incredibly important part of intellectual property law, the DMCA must be amended to provide for a greater number of easily navigable exemptions for software security research, to ensure that the integrity of our digital systems is protected for years to come.

Copyright Law in the United States and the DMCA

Copyright law in the United States is intended to encourage the creation of art and culture by rewarding authors and artists with a set of exclusive rights, and has a long and complicated history dating back to colonial times. It was first established with the federal Copyright Act of 1790. Since then, Congress has amended federal copyright law numerous times, with the DMCA being the latest major amendment [1].

The DMCA focuses on digital media, which was largely ignored in previous copyright laws. It prohibits the creation and spread of technology, devices, or services that are meant to violate the copyright of protected works. It also criminalizes the act of circumventing an access control, and heightens the penalties for copyright infringement on the internet [2]. The law was
first enacted to implement two international treaties created by the World Intellectual Property Organization (WIPO).

**The DMCA is Broken**

For security researchers, the problematic section of the DMCA arises in Section 1201 of the law. The original text of prohibits anyone to “circumvent protection afforded by a technological measure”, where such a measure is any technology incorporated into a copyrighted work that is meant to hinder unauthorized access to the work (access controls), and anyone from violating the copyright of the work (copy controls). In the case of software, these methods may include circumventing encryption, trusted platform modules (TPMs), or authentication requirements.

Importantly, good faith security testing by itself is not a violation of a copyright holder’s rights under the DMCA or any other U.S. copyright law. Security researchers only come into violation of the law when they bypass the measures designed to protect the copyright, not by performing the security analysis itself. Yet, as Bruce Schneier explains in *Click Here to Kill Everybody*, these measures mean that in effect it is illegal for anyone to “reverse engineer, locate, and publish vulnerabilities in software systems that protect copyright” [3].

All of these measures serve to protect the integrity of the software and hardware of the computing device, not just the copyright of the original creator. But, despite the reasonable justifications for software vendors to utilize these technologies to protect their works, their inclusion is ultimately harmful if security researchers are not allowed to lawfully circumvent them. It is well documented that software developers use the DMCA as a legal threat against security professionals, as companies such as Adobe, HP and Activision have all used it to pursue researchers auditing their products [3].

On the other hand, software companies contend that the protections of the DMCA are essential for protecting the security of their products. They argue that without the ability to achieve legal recourse for copyright violations, they will have no way to disincentivize bad actors from attempting to penetrate their products. In addition, they are concerned that security research that discloses any vulnerabilities found will give hackers a chance to exploit them
before they can be fixed [4]. While these are valid concerns, it is unclear whether evidence supports these assertions. In fact, there are cases where companies used the protections of the DMCA to deliberately conceal wrongdoing, as in the case of the 2015 Volkswagen emissions scandal.

**Case Study: Volkswagen 2015 Emissions Scandal**

In 2015, the United States Environmental Protection Agency (EPA) accused Volkswagen of illegally using software to cheat emissions standards. The agency alleged that the German automaker's vehicles used a sophisticated algorithm that was designed to undermine official emissions testing by engaging full emissions controls only during testing and disabling them afterwards, causing vastly more pollutants to emitted than legally allowed [5]. After this discovery, Volkswagen was slapped with a $2.8 billion dollar fine.

Researchers at West Virginia University discovered the deceptive code by developing a sensor system connected to the tailpipe of the vehicles. When the readings from these sensors did not match lab data, they had reason for concern and notified the EPA [6]. Why had nobody discovered it sooner? Simply put, the DMCA protected anyone from analyzing the software of the cars, where the issue would have been immediately apparent.

Simultaneously, the Library of Congress was in the process of considering proposed exemptions to the DMCA, including an exemption for security research known as “Proposed Class 22”. This class of exceptions would have allowed for “circumvention of TPMs [digital locks] protecting computer programs that control the functioning of a motorized land vehicle for the purpose of researching the security or safety of such vehicles” [7]. While this was supported by the software security community, it was opposed by the Alliance of Automobile Manufacturers, claiming that the proposal’s effect would be the opposite of its intention, “making American motorists, passengers, pedestrians and the general public less secure and more vulnerable” [7].

What lessons can policymakers, industry experts, and security researchers draw from this case? First, this example highlights how the DMCA protects software makers who are grossly in
violation of the law. If Volkswagen had to contend with security researchers auditing its code, it simply would not have been viable to commit this form of fraud. At the same time, it also shows how entrenched different industries are in opposing amendments to the DMCA. Even as a massive scandal unravelled its entire argument against the proposed exceptions, the Auto Alliance continued to claim that full DMCA protections were needed to preserve security in their vehicles.

Calls for Change

Software security researchers have been advocating for changes to this law for years now. Fearing legal consequences, they are unable to freely test copyrighted software that has copyright protection. Even though there exists an exemption process that involves permission of the software vendor, it is difficult, and very few companies are willing to give out such a license to interested auditors.

Thankfully, the Librarian of Congress granted a three year exemption for security testing in 2015, and renewed the exemption for an additional three years in 2018. This gives the security researchers the leeway needed to perform their work, without the interference of the industry. However, these exceptions do not go far enough in the eyes of many security researchers. In particular, advocacy groups like Rapid7 have called for “scaling back the requirement that all other laws and regulations be obeyed in order to qualify for the research exemption”, while Bruce Schneier says that the exemption is “temporary and still leaves a lot of room for harassment” [3]. In addition, the Library of Congress produces these rules on a three year cycle, and exemptions must be renewed every three years, creating a costly and distracting process for the security community [8]. Because of this, many in the software security community are advocating for a permanent solution that resolves the issues originated by the DMCA.

Short-Term Solutions

Currently, it is an extremely complex process to obtain or renew an exemption from the DMCA [9, 10]. While it is reasonable for the Copyright Office to deal with exemptions on copyrighted works with discretion, researchers who have legitimate purposes should not be
blocked by an overly complicated process. According to the Cyberlaw Clinic, a part of Harvard University’s Berkman Klein center, it takes approximately 575 hours of work for its attorneys, students, and interns to obtain an exemption [11]. In the short term, a better model is required to expedite the process.

One solution is to streamline renewals for existing exemptions. Currently, the United States Copyright Office, which is a division of the Library of Congress, expires all exemptions at the end of each three year period. For expiring exemptions, a streamlined process for renewal will prompt more security researchers to examine copyrighted software, leading to more security vulnerabilities being caught. In the streamlined model, a proponent of an exemption is required to file a request for renewal with evidence that this exemption should still be valid. For example, a proof of previously obtained exemption should be attached to the application. In the meantime, opponents of the exemption can also present evidence to the Copyright Office to prove why the renewal request should be declined. Depending on the evidence provided by both parties, the Copyright Office announces a final decision whether or not the renewal is valid [12]. This would be effective in the short term, as it requires little to no additional infrastructure to implement. Indeed, it would save resources for all parties involved, as both the Library of Congress and proponents for new exemptions would have to dedicate muchless time to producing and considering new proposals.

To help individuals go through the application process smoothly, the Copyright Office could offer a series of accessible services including legal consultation regarding any new DMCA policies so that applicants can get a more transparent view of the considerations the Copyright Office is facing. These consultants could provide advisory assistance and clarification of the rules before an applicant files a request. They would be responsible for handling individual cases and submitting it to the committee. With more support from the Copyright Office, the legally daunting task of achieving a DMCA exemption will become much more manageable for the security community.
Long-Term Solutions

In the long term, congress should reform the DMCA to include a strong list of permanent exemptions to protect all forms of security research. While the specifics are up for debate in the security community, there is consensus around several key points. This list of permanent exemptions can take a cue from the temporary exemptions granted in the last couple years. In October 2018, the Section 1201 exemptions were announced to allow an expanded list of exemptions based on the 2015 exemptions [11]. The new exemptions were expanded to smartphones and home appliances [13]. However, while enumerating different types of devices has been the norm in the past, it is not a sustainable solution for the future, as the types of new devices with software in them continues to increase. Congress should consider a blanket exemption for all types of software, as that would give the law the breadth needed to anticipate all potential devices that could be compromised. As the Internet of Things expands, computers will be embedded in all facets of our life, so exemptions from the DMCA should be expanded to software of all kinds, including medical devices, vehicles, and more.

In addition to changing what falls under the exception, the security community has rallied against specific language in the DMCA that states that researchers must “not violate any applicable law, including the Computer Fraud and Abuse Act of 1986” [14]. Removing this restriction would reduce much of the fear on the part of security researchers that they may face consequences for their research. While it would take a considerable amount of advocacy on the part of the security community to achieve such an amendment to the DMCA, it is worth the effort because software insecurity is a problem that will always persist.

Beyond the DMCA

Similar to the National Cyber Office (NCO) proposed by Schneier, a new federal agency for software security research can be established in the future [3]. The purpose of this agency would be to attract experienced security experts and grant them permission to conduct research on software products including copyrighted works with less restrictions. Eventually, the agency would consist of a group of researchers, a review committee who has the power to approve or deny a proposed project, and an implementation committee. With this model, researchers could
directly submit proposals to the committee for review, and upon permission of the committee, they would be able to conduct research free from the DMCA and other copyright laws. Furthermore, the agency would mainly focus on technology companies which have a large consumer base, and regularly check if any vulnerabilities exist in their software. Once researchers reach a final conclusion on a project, they would present a report to the implementation committee. The implementation committee would be responsible for informing the company of any existing security issues found in their software and enforcing the company to fix the issues in a certain amount of time depending on the scale of the problems.

The government can also consider collaborating with universities and partner institutions to help build a broader review community. In addition to setting standards about what are acceptable practices regarding software security, this research network would distribute the load of auditing the most critical and widely used software. By building the relationships, institutional support, and legal backing necessary for such a system, a much healthier and secure software ecosystem can be achieved.

**Metrics of Success**

As solutions to this problem are introduced and implemented, policymakers and security researchers alike will need a way of determining whether the changes were successful. The most obvious metric of success in this scenario is simply the number of DMCA takedown requests against security researchers. While DMCA takedown requests are generally not made public, some companies take it upon themselves to make that information available. For example, Github publishes every DMCA takedown that it complies with to an online repository, letting the public get a sense of how aggressively the DMCA is being used. While only a small subset of takedowns concern security testing, researchers can use this public data to find an indication of whether a solution is working or not. Likewise, Lumen is a public online database that collects and analyzes public takedown requests of online content. Importantly, the database contains entries for “millions of notices, some of them with valid legal basis, some of them without, and some on the murky border” [15]. As it collects data on unsuccessful takedowns as well, its data can give insight into whether corporate use of DMCA is akin to intimidating behavior towards
security researchers. As changes to the DMCA and surrounding copyright law are made, these public repositories will be the true measures of success.

**Next Steps**

Security research is beneficial to the people and the society, so the government should work toward a better environment for security researchers. In the short term, it is important to simplify the process for individuals to obtain and renew exemptions to reduce the burden on researchers. Although this is not the most preferable solution, streamlining the process of application and renewal is the most workable solution for the time being. Beyond that, expanding the list of exemptions is necessary as computer software is becoming more prevalent in an ever expanding Internet of Things. The rights of software users and researchers must be protected in response to the growing list of software products. In particular, security research for legitimate purposes must not be restricted by the DMCA and other copyright-related laws. These two solutions would have a positive effect on protecting user privacy of software products as well as getting companies’ attention on security issues of their products. However, while drafting and implementing these new rules, the laws of foreign countries should be considered as well. Copyright holders have an interest in enforcing their copyright oversees, and many copyright laws are based off of international agreements. Any broad change to the DMCA must take international considerations into account.

In this digital age, security research is becoming an increasingly important way to detect flaws in software and fix them. The failure to find vulnerabilities in software would cause great loss to the people and the society. Since the efforts of security researchers are critical in this process, they should not be taking the risks of possibly violating the DMCA and other copyright laws or intimidated by the overly-complex legal process. While focusing on protecting the rights of copyright owners, the Copyright Office should also be aware of the law’s negative effects on software security and seek new ways to encourage researchers with good intents.
References:

https://www.copyright.gov/title17/

https://www.copyright.gov/reports/studies/dmca/dmca_executive.html

[3] Click here to kill everybody.
https://www.schneier.com/books/click_here/

https://cdt.org/blog/the-current-dmca-exemption-process-is-a-computer-security-vulnerability/


http://time.com/4048115/volkswagen-golf-emissions-researchers/


https://blog.rapid7.com/2017/06/28/copyright-office-calls-for-new-cybersecurity-researcher-protections/


[12] Section 1201 of Title 17.  


https://lumendatabase.org/topics/1