Chicago-Kent Journal of Intellectual Property

Volume 22 | Issue 2 Article 2

4-20-2023

Security Researchers Battle Against the DMCA

Andre Sardaryzadeh

SECURITY RESEARCHERS BATTLE AGAINST THE DMCA

© 2023 ANDRE SARDARYZADEH*

Abstract

In the digital age, cybersecurity plays a principal role in resolving consumer concerns regarding data breaches. Nevertheless, United States copyright laws prohibit the effective use of cybersecurity tools that disrupt malicious hackers from gaining access to personal (and sensitive) information. One law, in specific, that is detrimental to the defense against malicious attackers is the Digital Millennium Copyright Act ("DMCA"). Specifically, section 1201 of the DMCA prohibits the circumvention of copyrighted information. Malicious hackers have various tools and techniques to obtain unauthorized access to personal information via software vulnerabilities. Importantly, these vulnerabilities often result in the theft of consumers' personal information; however, physical harm may also occur. Autonomous vehicles, for example, are ripe for software security concerns. Malicious hackers can and do attack safety-critical systems like engines and brakes.

Moreover, medical devices often have vulnerabilities in their software systems—leading to severe injury or death by, for example, implantable defibrillators. So, naturally, software systems have bugs that put consumer data at risk—otherwise, there would be no need for privacy policies. However, laws like the DMCA that hinder the activities of security researchers are counterintuitive to the remediation of these bugs (and consumer safety). On October 12, 1998, the U.S. Congress passed the DMCA, amending U.S. copyright law to address the relationship between copyright and the internet. Congress' reason for passing the DMCA was to address the concerns

*J.D. Candidate, May 2023, Roger Williams University School of Law. I want to thank Mr. Jerry Cohen, Adjunct Professor of Law at Roger Williams University School of Law and partner at Burns & Levinson, for his guidance throughout this process. I would also like to thank Dr. Afshin Sardaryzadeh, HMS Campus Information Security Officer, and Brittany N. Hatopp, MBA, for their reviews of this article.

of copyright holders who felt that there were too few protections for their work(s). Unfortunately, when writing the DMCA, Congress could not anticipate the rapid growth of technology and how ill-equipped the legal system is to keep up with technological advancements. Now, the DMCA overreaches its intended powers and subjects security researchers to criminal liability. The current technological climate calls for improved reliability and guidance regarding existing legal authorities, as well as how investigations should be held concerning security research. In addition, researchers are increasingly becoming independent and no longer affiliating themselves with institutions that housed them in the past (such as universities). This means they are moving away from restrictive research houses and opening to the public about vulnerabilities that would have previously been prohibited under contract—limiting those who can bring claims against researchers. Significantly, this is affecting the way inexperienced vendors go about handling reports. The connection between security research and certain consumer safety is where most of this argument lays its foundation. Public awareness of the benefits of security research will improve policy decisions, providing further understanding of contributions made to digital safety and security.

TABLE OF CONTENTS

I.INTRODUCTION 41
II.WHAT IS CYBERSECURITY? 44
A. Defining Cybersecurity 45
B. Cybersecurity Research 48
C. The Hunt for Vulnerabilities 49
III.DIGITAL MILLENNIUM COPYRIGHT ACT 52
A. History of the DMCA 52
B. Development of Section 1201 54
IV.NOTABLE INSTANCES OF THE "WORST" CRIMINAL CHARGES AGAINST SECURITY RESEARCHERS 58
A. *United States v. Elcom Ltd.* 59
B. The Kill Switch Discovery 61
V.REACTION TO GROWTH: CFAA VS. DMCA 63
A. *Van Buren v. United States* 65
B. *Green v. United States DOJ* 67
1. D.C. Circuit Court Rejects First Amendment Challenges 68
2. Non-Applicability of the Administrative Procedures Act 71
VI.SUGGESTIONS GOING FORWARD 72
A. Short-Term Solution 73
B. Incentivizing Ethical Hackers 74
C. Proposed Safe Harbor 75
D. Unraveling Benign & Malicious Hackers 77
E. Rethinking Who Governs the DMCA 78
VII.CONCLUSION 82

"An organization's understanding of the value of security and privacy and their willingness to treat cybersecurity as an essential part of the business are the most important organizational elements that need to be in place to deploy cyber professionals to identify and prevent cyber threats."[1]

1. Afshin Sardaryzadeh, Identifying Effective Cybersecurity Team Behaviors In Order to Transform Cybersecurity (Dec. 14, 2017) (unpublished Ph.D. dissertation, Brandman University) (on file with author).

I. INTRODUCTION

There are currently more than four billion people in the world connected to the internet.[2] As such, cybersecurity is one of the most pressing subjects for large, medium, and small-sized companies. Importantly, the risk of cyber-attacks has steadily grown due to our increased reliance on computers, smart devices, the internet, and wireless network standards, causing major concerns for all. Since 2020, the average cost of a data breach has increased 12.7% from $3.86 million to $4.35 million in 2022.[3] Not surprisingly, the average cost of a data breach in the media industry stands at $3.15 million in 2022.[4] One cost that continues to have a devastating impact on a company's growth is the law concerning copyright infringement in cyberspace. Currently, the copyright infringement laws protecting digital devices conflict with security research. The reason why these restrictions on security research cause discomfort is simple: they harm legitimate security research that would benefit consumers.[5]

On October 12, 1998, the U.S. Congress passed the Digital Millennium Copyright Act ("DMCA"), amending U.S. copyright law to address the relationship between copyright and the internet.[6] Congress's reason for passing the DMCA was to address the concerns of copyright holders who felt that there were too few protections for their works.[7] Under the DMCA, it is "a criminal act to produce and disseminate devices, services, or technology that evades measures that control the access to copyrighted works."[8] Before Congress passed the DMCA, "the World Intellectual Property Organization ("WIPO") treaties were the [building block] for the U.S. Legislation."[9]

Congress, in attempting to keep up with the growth of technology in the digital age, implemented the WIPO treaties via passing the DMCA to address former treaty obligations not thoroughly analyzed under existing U.S. law.[10] To implement U.S. treaty obligations, certain prohibitions relating to the circumvention of technological protections were created. Specifically, "[l]egal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their

2. *Digital Around the World*, DATAREPORTAL (July 7, 2022), https://datareportal.com/global-digital-overview [https://perma.cc/VKD9-3ARZ] (stating that 5.16 billion people around the world are on the internet—"equivalent to 64.4% of the world's total population").

3. IBM Corporation, Cost of a Data Breach Report 2022(July 2022),https://www.ibm.com/downloads/cas/3R8N1DZJ [https://perma.cc/99H6-654E].

4. IBM Corporation, *supra*, note 3 (defining "media" as television, satellite, social media, and internet).

5. Harley Geiger, *Thawing Out the Chilling Effect Of DMCA Section 1201*, RAPID7 BLOG: PUBLIC POLICY (Nov.15, 2021),https://www.rapid7.com/blog/post/2021/11/15/thawing-out-the-chilling-effect-of-dmca-section-1201/ [https://perma.cc/YWK6-SBU3].

6. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. §§ 1201–1202 (2012)) (starting the development of legal punishments regarding infringements of copyrighted digital works); U.S. Copyright Office, *The Digital Millennium Copyright Act*, https://www.copyright.gov/dmca/ [https://perma.cc/NR3Y-AAE4] (last visited Nov. 27, 2022).

7. *History and Overview of the DMCA*, FINDLAW (Apr. 4, 2016), https://www.findlaw.com/smallbusiness/intellectual-property/history-and-overview-of-the-dmca.html [https://perma.cc/QJ59-6HF4].

8. *History and Overview of the DMCA*, *supra* note 7.

9. U.S. Copyright Office, *Executive Summary Digital Millennium Copyright Act*, COPYRIGHT.GOV https://www.copyright.gov/reports/studies/dmca/dmca_executive.html [https://perma.cc/8SZM-Y5BE] (last visited Sept. 17, 2022).

10. *Id*.

works, and against the removal or alteration of copyright management information" were established.[11] Now, "the DMCA focuses [primarily] on anti-circumvention laws" that penalize "unauthorized users who circumvent or hack copyrighted technology or software."[12] Circumvention is the act of "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological [protection] measure . . . ."[13] More simply stated, circumvention of technological protection measures ("TPM") are tools that allow a user to evade software that blocks or limits access to work or specific actions concerning the work (e.g., copying). TPMs are licensing protocols—serial numbers, keygens, passwords, and other methods to prevent the hacking of a software.[14]

Although the intent of the DMCA is justifiable—to protect intellectual property rights—its current framework poses a significant risk to researchers. By invoking the DMCA, vendors can prevent publicizing damaging or embarrassing research. Specifically, Section 1201 of the DMCA has caused the most discomfort for cybersecurity professionals. Section 1201 of the DMCA provides several anti-circumvention mandates, including the "circumvention of technological measures" 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."[15] In other words, DMCA Section 1201 restricts security research on software programs without obtaining authorization from the owner of the copyrighted software. The effect of this regulation even extends to software found on devices the researchers own.

Before their most recent updates, the U.S. Copyright Office (referred to as the "Office" or "Copyright Office") broadly applied DMCA's security research exception. However, the Office only offered legal protection from Section 1201 to researchers who complied with "every other law or regulation in the whole world, no matter how obscure."[16] The term "obey all other laws" was extensively debated. On July 14, 2021, Harley Geiger,[17] Prof. J. Alex Halderman,[18] and Blake Reid[19] (collectively referred to as the "Advocates") met with Kevin Amer and Brad Greenberg of the Copyright Office to discuss the exemption petition for Security Research. The meeting focused on several issues; relevant here was the "any applicable law" provision of the 2018 security research exemption.

11. *Id.*

12. *See* Katherine Weigle, *How the Digital Millennium Copyright Act Affects Cybersecurity*, 9 AM. U. INTELL. PROP. BRIEF 1, 3-4 (2018) (arguing that security researchers should be allowed to break into electronic devices through circumvention).

13. 17 U.S.C. § 1201 (b)(2)(A) (2018) (focusing on additional violations regarding the circumvention of technological measures).

14. Dan Goodin, *Trusted platform module security defeated in 30 minutes, no soldering required*, ARS TECHNICA (Aug. 3, 2021), https://arstechnica.com/gadgets/2021/08/how-to-go-from-stolen-pc-to-network-intrusion-in-30-minutes/ [https://perma.cc/H63R-C7SS].

15. Geiger, *supra* note 5 (referring to circumvention of copyright protection systems, 17 U.S.C. § 1201).

16. *Id.*

17. Harley Geiger was the Advocacy Director and Senior Counsel at the Center for Democracy & Technology—working on issues such as civil liberties and government surveillance, computer crime, drones, and cybersecurity.

18. Professor of Computer Science & Engineering, University of Michigan.

19. Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law, counsel to Prof. Halderman.

The Advocates argued that the limitation had harmful effects on security researchers by purportedly stripping them of the safe harbor exceptions. If a security researcher inadvertently violated laws with significant grey areas (e.g., the Computer Fraud and Abuse Act of 1986), minor laws unrelated to security (like the electrical code), or sweepingly restrictive foreign laws, they would lose liability protection under Section 1201.[20] The Advocates offered alternative language that would turn the requirement of compliance with all applicable laws into an essential reminder that these other laws may still apply.[21] Subsequently, in October 2021, the Copyright Office adopted the alternative language and removed the "all other laws" requirement. The new terminology is of particular interest to technology-based companies because it allows for the circumvention of TPMs on all devices and machines (not including gaming consoles) to investigate potential violations of licenses for "free and open source software [("FOSS")]."[22]

Still, all such investigations must be performed on a legally obtained device and cannot violate other laws. An investigation must be conducted by (or on behalf of) a party who has standing to bring a breach of license or copyright claim. The claim must be made via a good faith[23] belief that such an investigation is necessary given the breach.[24] Moreover, the investigation must only be conducted to investigate potential infringement(s). Because of the new (i.e., updated) exemption adopted in 2021, independent security research has obtained more significant and more justifiable legal protections.

In summation, section 1201 of the DMCA makes it illegal to circumvent technological protection measures (TPMs) that control access to copyrighted works. This includes bypassing software that restricts access to devices, systems, or applications. The law has implications for security researchers, as TPMs may be present in the software or systems they want to investigate to identify vulnerabilities or security flaws. If they bypass the TPMs, they could be liable under Section 1201, even if they intend to improve security. This can create a chilling effect on security

20. U.S. Copyright Office, *Ex Parte Communications Guidelines*, U.S. COPYRIGHT OFFICE (2021) https://www.copyright.gov/1201/2021/ex-parte-communications.html [https://perma.cc/EGA5-HZNG] (reasoning that "non-US laws are not the only cause of ambiguity for researchers, and that there continues to be substantial overlap and ambiguity in domestic law." For example, the Computer Fraud and Abuse Act after the Supreme Court's *Van Buren* ruling, as well as swiftly evolving privacy laws. The Office stated that the "any applicable law" provision continues to cause adverse effects on good faith security research because of the broad, ambiguous, and constantly changing applicability of other laws).

21. *Id.* (Striking: "and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code." Inserting:

> "Good-faith security research that qualifies for the exemption under paragraph (b)(16)(i) of this section may nevertheless incur liability under other applicable laws, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code, and eligibility for that exemption is not a safe harbor from, or defense to, liability under other applicable laws.").

22. John Kind, *Important New Exemptions to the Copyright Law's Anti-circumvention Provisions*, JDSUPRA (2022) https://www.jdsupra.com/legalnews/important-new-exemptions-to-the-4928873/ [https://perma.cc/4ZGZ-D4Z2].

23. *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act*, DEPARTMENT OF JUSTICE (May 19, 2022), https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act [https://perma.cc/BZJ7-WXJK] (providing that "[g]ood faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm.").

24. Kind, *supra* note 22.

research and limit the discovery and reporting of security vulnerabilities, as researchers may be afraid to investigate specific systems for fear of legal consequences. So, although the current protections for security researchers are now stronger under DMCA Section 1201, the legal risk for security researchers continues at a hindering level. This article analyzes the role of cybersecurity and ways to streamline U.S. computer crime laws, specifically the DMCA Section 1201.

II. WHAT IS CYBERSECURITY?

The Cybersecurity & Infrastructure Security Agency ("CISA") defines cybersecurity as being "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[25] In other words, cybersecurity is a system of defenses put in place to protect people, devices, processes, and technologies from malicious attacks and unintentional damage—protecting, for example, web-associated systems, hardware, software, and information, from cyber dangers.[26] Although the definition of cybersecurity can be understood in many ways, the common denominator is that it is a protective measure used across many industries.

Think of a computer network like a house. In that house, the owner stores things that are valuable to them, just as a network of systems store data that is valuable to the company or organization. Moreover, that same homeowner may not want a person walking into their house randomly, especially if the person is unauthorized and is likely to take or damage the homeowner's valuables or cause financial loss. Cybersecurity experts, like homeowners, also put controls in place to prevent unauthorized entry and investigate any forced breaches.

Alternatively, cybersecurity can also be analogized to the system by which the human body keeps itself healthy. This perspective focuses on internal monitoring, reducing risky behavior, eliminating vulnerabilities, defending the perimeter, and monitoring the ways in which malicious actors get in. A cybersecurity system composed of cybersecurity experts and specific tools keeps the organization, or body, healthy continuously. Sometimes, however, organizations utilize new tools or systems without proper planning and thinking about how those new tools or systems will affect the cyber defenses already in place. This strategy gives up the home-field advantage of having detailed knowledge of one's own systems and

25. *What is Cybersecurity?*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Nov. 14, 2019), https://www.cisa.gov/uscert/ncas/tips/ST04-001 [https://perma.cc/AHB5-GSSD].

26. *See* Rudy Takala, *Rep. Lieu Demands Answers on Weak Federal Cybersecurity*, WASH. EXAMINER (Sept. 28, 2016, 12:45 PM), http://www.washingtonexaminer.com/rep-lieu-demands-answers-onweak-federal-cybersecurity/article/2603089 [https://perma.cc/NR2Z-B78H] ("A congressional leader on cybersecurity is seeking to find out why federal agencies have failed to implement measures that would improve their cybersecurity posture against the growing volume of cyberattacks against government."); Craig Timberg, *Lawmakers Demand Accounting from Equifax on Massive Security Breach*, WASH. POST (Sept. 11, 2017), https://www.washingtonpost.com/business/technology/lawmakers-demand-accounting-from-equifax-on-massive-security-breach/2017/09/11/733ddf58-9728-11e7-82e4-f1076f6d6152_story.html [https://perma.cc/9C55-XFZU] ("A sternly worded letter from the top Republican and Democrat on the Senate Finance Committee included a list of 13 questions intended to illuminate the murky circumstances surrounding the breach[.]" That letter included the data that was exposed, how the hack was detected, and whether the company has systems adequate for detecting and thwarting).

data.[27] Although security teams usually trust new tools, it's the job of security researchers to validate that such tools do not have open vulnerabilities or weaknesses. This is an example of the important role security researchers play, though that role may sometimes conflict with laws such as the DMCA.

The role cybersecurity experts, teams of technicians, engineers, and architects play in creating an ecosystem of defense cannot be understated. "All truly effective security organizations are made up of tinkers and thinkers, yearning to create, to improve, and to plant seeds that will grow to change the world."[28]

A. Defining Cybersecurity

Defining cybersecurity is tricky. People have come to rely on soundbites from policymakers and the press when citing their definitions of cybersecurity. Although policymakers and the press may not be wrong, that does not mean they are altogether right.

In short, cybersecurity is the system and processes put in place that keep digital content secure and safe from cyber-attacks and malicious threats. Users rely on a collection of practices, people, and tools to protect their networks, computers, and other devices from those who want to steal their data or disrupt the device's functionality. In the private sector, cybersecurity is often recognized in relation to data breaches.[29] Indeed, significant resources are dedicated to funding security experts tasked with aiding companies in their efforts to prevent data breaches and remediate the effects of a breach. The worldwide cybersecurity industry generated an estimated $173.5 billion in 2022.[30] Companies are justifiably concerned about the personally identifiable information exposure of their consumers, customers, and employees. Additionally, data breaches tend to lead to leaks in a company's trade

27. *See* Julianne Basinger, *A Campus Culture of Cybersecurity The Chronicle of Higher Education* (2019), https://focus.vpfinance.virginia.edu/sites/focus.vpfinance/files/2019-11/Campus%20Culture%20of%20Cybersecurity.pdf [https://perma.cc/9QDQ-NYQW] (quoting Dr. Afshin Sardaryzadeh on creating a cybersecurity culture: "Creating a culture of cybersecurity requires identifying a higher-education institution's top information-security risks and then crafting communications strategies that are tailored to the personal and professional needs of individual students, faculty, and staff members.").

28. Billy Yost, *Dr. Michael Sardaryzadeh: Wave Spotter*, PROFILE (Mar. 15, 2021), https://profilemagazine.com/2021/michael-sardaryzadeh-texas-am/ [https://perma.cc/ND9T-TK9T].

29. *See* U.S. Government Accountability Office, *GAO-06-672 Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan* (June 16, 2006), https://www.gao.gov/assets/gao-06-672.pdf [https://perma.cc/2YU5-UYWK]. ("The diffuse control of the [i]nternet makes planning for recovering from a disruption more challenging." Certain areas "of the [i]nternet are controlled by government organizations, while others are controlled by academic or research institutions." Nevertheless, most of the internet, as it stands, is owned, and operated through the private sector. "Each organization makes decisions to implement or not implement various standards based on issues such as security, cost, and ease of use.").

30. *The worldwide cyber security industry is projected to reach $266 billion by 2027*, GLOBENEWSWIRE NEWS ROOM (Sept. 22, 2022), https://www.globenewswire.com/en/news-release/2022/09/22/2520978/28124/en/The-Worldwide-Cyber-Security-Industry-is-Projected-to-Reach-266-Billion-by-2027.html [https://perma.cc/EQP9-E9GM]; *see Norton Cyber Security Insights Report* (2016), https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/2016-Norton-Cyber-Security-Insights-Report.pdf [https://perma.cc/5AKF-K8SW] (providing statistics on cybersecurity breaches as reported by Norton Software Company); *see also* Houlin Zhao, *Internet Security Threat Report 2015*, SYMANTEC (June 11, 2015), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf [https://perma.cc/8NVQ-6XHX] (providing cybersecurity threat trends in 2014).

secrets, intellectual property, or other confidential business information. These leaks can cause severe financial and reputational losses to the company.

Notably, data theft is only a single subsection of cybersecurity. Another related task of cybersecurity professionals is to prevent the destruction or inaccessibility of data. Ultimately, "cybersecurity involves the *protection* of networks, systems, and data from damage."[31] Its aim is "to safeguard the confidentiality integrity, *and* accessibility of data (commonly known as the "CIA" triad)."[32] Data destruction, whether done by well financed criminal organizations in retaliation for non-payment of ransomware or for industrial or nation-state competition, is a real cyber, or internet-based, threat to governments and organizations alike.

In the United States, internet-based crimes have become one of the fastest-growing security threats. The rise of internet usage gives way to "a shift in how people use computers for transactions and communication."[33] Hackers utilize personally identifiable information[34] ("PII") to commit, for example, identity fraud. Information that directly identifies a person can consist of names, addresses, social security numbers, or other identifying numbers or codes, telephone numbers, email addresses, etc.[35] The United States was the target of approximately forty-six (46) percent of all cyberattacks in 2020—that is more than double the amount of attacks on any other country.[36] Generally, people have become aware of the increasing risks associated with cybercrime. It is evident that the United States, for many reasons, is one of the biggest targets of criminally initiated internet-based crime.

Cybersecurity is vital in government, military, corporate, financial, and medical industries. These industries "collect, process, and store unprecedented amounts of

31. Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401 (2016). Available at: http://digitalcommons.chapman.edu/chapman-law-review/vol19/iss2/3.

32. *Id*. (citing Jonathan Freedland, *US news from the Guardian*, THE GUARDIAN (Jan. 2, 2015), http://www.theguardian.com/us-news/ 2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview).

33. Ani Petrosyan, *U.S. Consumers and Cyber Crime*, STATISTA (July 6, 2022), https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/ [https://perma.cc/QVX6-HSR8].

34. *Explore Terms: A Glossary of Common Cybersecurity Terminology*, NAT'L INITIATIVE CYBERSECURITY CAREERS & STUD., www.niccs.us-cert.gov/glossary [https://perma.cc/2KAX-7L2P] (defining Personally Identifiable Information as "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."); *see Guidance on the Protection of Personal Identifiable Information*, U.S. DEPARTMENT OF LABOR https://www.dol.gov/general/ppii [https://perma.cc/BZ3Z-QA6X] (providing that PII is "[a]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.").

35. *Id*.

36. John Lambert, *Microsoft Digital Defense Report shares new insights on nation-state attacks*, MICROSOFT SECURITY BLOG (Oct. 25, 2021), https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/ [https://perma.cc/WC7A-MVQW] (stating that The Microsoft Threat Intelligence Center and the Microsoft Digital Crimes Unit have observed that nearly 80 percent of nation-state attacks were directed against government agencies, think tanks, and non-government organizations.); *See also* Ani Petrosyan, *U.S. consumers and cyber crime*, STATISTA (2022), https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/#:~:text=In%20a%20September%202018%20survey,been%20hacked%20more%20than%20once [https://perma.cc/9W6F-E2U2] (last visited Dec 6, 2022) (releasing a statistic that 32.7% of U.S. residence suffered a hack of their social media or e-mail account).

data on computers and other devices."[37] As stated, the types of stored data can range from intellectual property to PII. Unauthorized access or exposure to that data could result in irreparable harm. Moreover, as "the volume and sophistication of cyberattacks grow, companies . . . need to take steps to protect their sensitive business and personal information."[38] Presently, stolen, or compromised credentials are the primary attack vectors in 19% of breaches.[39]

An annual report published by the Theft Resource Center in August 2022 found 817 cases of individuals impacted by data compromises in the United States.[40] Furthermore, a study—conducted by Ponemon Institute, sponsored, analyzed, and published by IBM Security—shows that the United States has the highest average total cost of a data breach at $9.44 million, a 4.3% increase from 2021.[41] Although the United States is not alone in the millions group, the country with the closest average cost is Canada, totaling $5.64 million. Cyberattacks are not only financially harmful,[42] but they can also lead to closer regulatory oversight and reputational damage.

Regulatory laws like the U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[43] and the E.U. General Data Protection Regulation ("GDPR")[44] require any organization that stores patient or customer data to have relevant security processes and technologies in place. HIPAA, for example, involves using identity and access control systems in addition to encryption.[45] The

37. Juliana De Groot, *What is Cyber Security? Definition, Best Practices & Examples*, DATAINSIDER (June 10, 2022) https://digitalguardian.com/blog/what-cyber-security [https://perma.cc/4YBF-RXL6].

38. *Id*.

39. Cost of a Data Breach Report 2022, *supra* note 3.

40. Lynn Hulsey, *U.S. Sees Decrease in Data Breaches In First Half of 2022*, GOVERNMENT TECHNOLOGY (Aug. 29, 2022), https://www.govtech.com/security/u-s-sees-decrease-in-data-breaches-in-first-half-of-2022; *See also Data breaches and individuals impacted U.S. 2022*, STATISTA (Aug. 31, 2022), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://perma.cc/8TXU-2HE7].

41. Cost of a Data Breach Report 2022, *supra* note 3.

42. Ramya Mohanakrishnan, *What is cybersecurity? definition, importance, threats, and best practices*, SPICEWORKS IT SECURITY (2022), https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cybersecurity/ [https://perma.cc/5J42-W82M] (proving related legal, regulatory, and brand reputation concerns must be addressed).

43. Health Insurance Portability and Accountability Act of 1996 § 1173 (The Health Insurance Portability and Accountability Act of 1996 is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge); *see also* 45 C.F.R. §§ 164.302–.318 (2016) (outlining the Department of Health and Human Services' security-standard regulations authorized by HIPAA—requiring health plans, healthcare, clearinghouses, healthcare providers, and their business associates to adopt "administrative, technical, and physical safeguards" to protect PII related to health information).

44. In 2018, the European Union's General Data Protection Directive ("GDPR") went into effect. The GDPR is the most developed, and thought out, privacy and security law in the world. Although it was drafted and passed by the European Union, its obligations stretch onto organizations everywhere, so long as they target or collect data related to people in the EU. The regulation came into effect on May 25, 2018. The GDPR levies harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. *See* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 99, 2016 O.J. L 119/1.

45. *Cloud Computing*, HHS.GOV (Oct. 6, 2016), https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html [https://perma.cc/4GB9-DV84].

consequence of noncompliance may result in civil or criminal penalties—and opening the door to lawsuits against companies.[46] Compliance with these requirements provides "[a] well-implemented cybersecurity blanket allow[ing] companies to offer their most essential services even through outages and natural disasters."[47]

Therefore, more emphasis must be placed on methods to keep cybercriminals from hacking into accounts and systems to collect sensitive information. However, the emphasis on cybersecurity is not only found at the corporate level but is equally important across all industry verticals. For example, the Department of Homeland Security is taking steps to "strengthen cybersecurity resilience across the nation" by taking on the threat of ransomware through "a more robust and diverse workforce" that includes a series of 60-day sprints to optimize public awareness.[48]

B. Cybersecurity Research

If it was not clear above, cybersecurity is a national (and global) priority. Yet, vulnerabilities continue to be exploited at an alarming rate, thereby undermining national security, critical cyber infrastructure[49], and personal privacy.

Cybersecurity research is a fast-growing area whereby researchers from institutions across the country and globe conduct research on the state of security of devices and systems from large-scale computers to smaller Internet of Things ("IoT"). IoT examples include wearable devices designed for the human body. IoT saw extreme growth within the last decade, thus creating greater risk because of "consumer products [being] widely used in daily life, ranging from automobiles to medical devices to thermostats and home appliances. . . ."[50] In addition, the devices connecting to the internet create vulnerabilities open "to remote manipulation, exploitation, and attack."[51] Cyber-attacks affect not just livelihood but life as well. This has been documented through compromised medical devices and medical IoTs

46. *What Is HIPAA Security Rule and Privacy Rule?*, TRELLIX (last visited Dec. 7, 2022) https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-hipaa-security-rule-and-privacy-rule.html [https://perma.cc/QJB6-BN6F].

47. Mohanakrishnan, *supra* note 42.

48. *Cybersecurity*, HOMELAND SECURITY (Nov. 1, 2022), https://www.dhs.gov/topics/cybersecurity [https://perma.cc/9FEN-4JYW].

> President Biden has made cybersecurity a top priority for the Biden-Harris Administration at all levels of government. To advance the President's commitment, and to reflect that enhancing the nation's cybersecurity resilience is a top priority for DHS, Secretary Mayorkas issued a call for action dedicated to cybersecurity in his first month in office. This call for action focused on tackling the immediate threat of ransomware and on building a more robust and diverse workforce.

49. *Infrastructure security*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY https://www.cisa.gov/infrastructure-security [https://perma.cc/7WVJ-L8QZ] (last visited Nov. 15, 2022) (critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security).

50. Deirdre Mulligan et al., *Cybersecurity Research: Addressing the Legal Barriers and Disincentives*, UC BERKELEY SCHOOL OF INFORMATION (Nov. 30, 2022), https://www.ischool.berkeley.edu/research/publications/2015/cybersecurity-research-addressing-legal-barriers-and-disincentives [https://perma.cc/QQ23-T2G8].

51. *Id*. at 2 (active investigations and subsequent disclosures are the best way to patch these vulnerabilities. Unfortunately, researchers are hesitant to engage in remediation due to the issues "of liability risks associated with security research[, which are] well known within the computer science and related legal community").

such as defibrillators, CT-scanners, heart monitors, and pacemakers.[52] The danger to life becomes even greater with the increase in autonomous vehicles that are connected to networks and have been proven to contain vulnerabilities.[53] Therefore, it is of increasing importance that the security of these devices is assessed often and through as many methods as possible, by security researchers.

Cybersecurity research aims to understand the nature of vulnerabilities and exploits to harden operating systems and, more interestingly, the many devices that make up the Internet of Things. It is in the physical world, as opposed to the cyber world, where cybersecurity research is tangibly appreciated.[54] The multitude of research being conducted in the cybersecurity arena continuously adds to the greater good and reduces the billions lost to all manner of cyber-attacks.

Another area where security research is of paramount importance is cyber warfare. The term "warfare" is usually associated with soldiers in battle; in this context, it refers to the malicious acts taken to attack and damage computers or information networks.[55] Generally, cyber warfare "involves the actions [taken] by a nation-state or international organization . . . ."[56] Some examples of cyber warfare include espionage, sabotage (sometimes of connected devices), Denial-of-service ("DoS") attacks, electrical power grid and other critical infrastructure comprises, propaganda attacks, economic disruption, and more.[57] Cyber warfare is a genuine and severe threat affecting national safety and businesses' privacy.[58]

C. The Hunt for Vulnerabilities

The classic American animated cartoon series *Scooby-Doo, Where Are You!* is about a group of friends and their talking Great Dane, Scooby-Doo, driving around

52. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 130 (2014) (stating that "Jay Redcliffe, a security researcher with diabetes" showed how insulin pumps are remotely accessible and can be "controlled by a hacker near[] the device's user." The consequence of this could result in a malicious hacker "caus[ing] a monitor to display inaccurate information, causing a diabetic patient to mis-administer" their unique insulin dosage) (citations omitted).

53. Barry Sheehan et al., *Connected and Autonomous Vehicles: A Cyber-Risk Classification Framework*, 124 TRANSP. RSCH. PART A: POL'Y AND PRACTICE 523–536 (June 2019); Holden Benon, *A Peek under the Hood: Why Lawmakers Should Strengthen the Current DCMA Exemption for Security and Safety Research into Car Software*, 15 HASTINGS BUS. L.J. 155 (Winter 2019) (stating that "independent researchers in West Virginia discovered that Volkswagen cars contained certain software" allowing it to "deceive emission tests." Not surprisingly, "Volkswagen secretly programmed their vehicles' software to enable . . . dece[ption during] emissions tests.") (citations omitted).

54. Importantly, security by obscurity—the assumption that a vulnerability can be kept hidden and resolved before malicious actors find it and exploit it—has been proven to faulter. This method of "security" is specifically ill-suited for the world as it is today.

55. *Cyber Warfare*, RAND, https://www.rand.org/topics/cyber-warfare.html [https://perma.cc/8CSA-YQZ7].

56. *Id*.

57. *Id*.

58. Duane Chambers, *What Is A Security Researcher?*, MEDIUM (Oct. 19, 2021), https://duanechambers77.medium.com/what-is-a-security-researcher-ef303942cc65; *see* Jim Finkle, *Target cyber breach hits 40 million payment cards at holiday peak*, REUTERS (Dec. 19, 2013), https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219 (describing the incident with Target Corp. where credit and debit card information was stolen from about 40 million shoppers).

in the Mystery Machine in search of out-of-this-world mysteries to solve.[59] Even when they are not actively looking for mysteries, the gang still has a way of finding themselves in the center of one, and it is up to them to solve it.[60] Similarly, in cybersecurity, security researchers are professionals who are consistently finding vulnerabilities in systems, investigating why the vulnerabilities happen and properly reporting their findings to assist in ultimately patching and remediating vulnerable systems.[61] Like Scooby-Doo and his friends, security researchers are the ever-curious good guys keeping people (and companies) safe from malicious actors.

As the cybersecurity world grows and more data leaks occur, a security researcher's job is to keep abreast with modern technology trends and the latest data developments. Typically, these people are responsible "for investigating malware, analyzing and understanding their capabilities, documenting the incidents of compromise (IOCs)," and implementing the best practices to mitigate the threat.[62] Additionally, with the computer skills and technical knowledge of experts in their field, security researchers identify cybersecurity vulnerabilities within an organization and attempt to resolve those issues quickly. In other words, because security researchers have specialized industry expertise, they not only understand the remediation paths to vulnerabilities that they find but are also able to correlate their findings with similar systems and devices to predict future ones.

Security researchers must dedicate a considerable amount of their resources to properly performing their roles to analyzing source code and malware and reviewing company incident reports to better comprehend the threat(s). Malware, specifically, is the biggest challenge. In these scenarios, "[p]atience and strong analytical skills" are required "to disassemble [the] malware, reverse engineer[ ] it to know how it works, and design mitigation[techniques]."[63] In addition, there is the reality that an increase or propagation in malware can also occur from the repackaging and remanufacturing of an existing threat. Therefore, security researchers need to deploy cost- and time-effective strategies.

In web-based security or the larger arena of cyber warfare, knowing who the opposition is (i.e., the malicious actor) becomes essential in tracking the individual's methods. As such, security researchers often get in the mind of their enemies and simulate the efforts of real-life cyber-attackers. This practice is referred to as penetration testing or red team activity.[64] In these cases, tools and strategies are employed to actively investigate a company's functioning applications with

59. *See* Longo v. Good Shepherd Child Care Ctr., No. 3:14cv181, 2014 U.S. Dist. LEXIS 114668, at *1 n.2 (M.D. Pa. Aug. 19, 2014) ('"Scooby-Doo is an American animated cartoon franchise [about] four teenagers . . . and their talking Great Dane dog named Scooby-Doo, who solve mysteries involving supposedly supernatural creatures through a series of antics and missteps." http://en.wikipedia.org/wiki/Scooby_Doo (last accessed Aug. 15, 2014)').

60. Good Shepherd Child Care Ctr., No. 3:14cv181, 2014 U.S. Dist. LEXIS 114668, at *1 (M.D. Pa. Aug. 19, 2014) ('. . . the minor plaintiff watched "Scooby Doo" cartoons before her naps at the daycare center and may have heard them while restrained in her bed . . . .' These cartoons gave her nightmares, which she continues to have to this day.').

61. *What is a Security Researcher & How can I become one?*, CYBERTALENTS BLOG (2022) https://cybertalents.com/blog/what-is-a-security-researcher-how-can-i-become-one [https://perma.cc/8BKH-AAFR].

62. *Security researcher*, BUGCROWD (2022), https://www.bugcrowd.com/glossary/security-researcher/ [https://perma.cc/SD5C-RUZ2].

63. *Id*.

64. *Red Team*, FORTRA (April 10, 2023) https://www.coresecurity.com/penetration-testing/red-team [https://perma.cc/2M73-6KCB].

penetration tests to locate any possible security vulnerabilities that hackers may attempt to exploit.[65] Security researchers are essential in identifying vulnerabilities in digital technologies and increasing awareness of those vulnerabilities.

Vulnerability reporting is important in the many steps needed for a full defense. Vulnerability reporting outlines the activities that security researchers undertake—in a legally authorized manner—to find and properly report vulnerabilities located in internet-accessible systems and services. In practice, vulnerability reporting is the "act of initially providing vulnerability information to a party that was not believed to be previously aware."[66] The individual or organization performing the research is known as the security researcher, and is then considered the vulnerability reporter after disclosing the security threat.[67] Feedback received through this program or process allows the organization or device manufacturer to fix flaws quickly when possible, strengthening the integrity of the system or product to ensure the safety of customers and enhancing data protection.

The process begins by "evaluat[ing] if the system or product is susceptible to any known vulnerabilities" and then trying to identify or uncover any new vulnerabilities in those systems or products. Part of this activity includes providing threat levels for each vulnerability, then, in some instances the security researcher "recommends remediation or mitigation" tactics.[68] Programs for developing more robust vulnerability reporting policies have been created "by government agencies, including 18f, and CISA, who mandated that agencies begin setting them up."[69] These programs impose more responsibilities on security researchers when disclosing vulnerabilities in public-facing government tech.[70] CISA has stated: "Vulnerability disclosure policies enhance the resiliency of the government's online services by encouraging meaningful collaboration between federal agencies and the public."[71] Government agencies and institutions such as CISA and the National Institute of Standards and Technologies ("NIST") should contribute more resources to such collaboration programs between federal agencies, private firms, and the public. Making them more available would serve as a great model for companies

65. *Dynamic Application Security Testing (DAST) tools explained*, RAPID7, https://www.rapid7.com/fundamentals/dast/ [https://perma.cc/M5A9-KXNC].

> To address this growing threat, businesses are increasingly deploying DAST tools as part of a more security-forward approach to web application development. DAST tools provide insight into how your web applications behave while they are in production, enabling your business to address potential vulnerabilities before a hacker uses them to stage an attack.

66. Vulnerability disclosure policy, CFTC, https://www.cftc.gov/vulnerability-disclosure-policy [https://perma.cc/89EU-ZR55] (last visited Nov. 21, 2022).

67. *Id*.

68. Nik Hewitt, *What is Vulnerability Assessment | VA Tools and Best Practices*, IMPERVA (Nov. 30, 2022), https://www.imperva.com/learn/application-security/vulnerability-assessment/ [https://perma.cc/2DMF-FKYL] (e.g., if the cause of a vulnerability is an old version of an open source library, remediation would be to upgrade the library).

69. Nat Meysenburg, *Cybersecurity Research Should Not Be A Crime: Why We Need Clear, Permanent CFAA and DMCA Exemptions*, NEW AMERICA. (Nov. 18, 2021), https://www.newamerica.org/oti/briefs/cybersecurity-research-should-not-be-a-crime/ [https://perma.cc/R29N-RLE2].

70. *Id*.

71. *Id*.; *see Binding operational directive 20-01 - develop and publish a vulnerability disclosure policy*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Sept. 2, 2022), https://www.cisa.gov/binding-operational-directive-20-01 [https://perma.cc/3L3U-KH5J] (making it easier for the public to know where to send a report, what types of testing are authorized for which systems, and what communication to expect).

and security researchers to use as guidance. After all, the more collaboration between well-intentioned cybersecurity teams and experts, the harder it will be for malicious attackers.

Laws suppressing the use of security software and tools, like Dynamic Application Security Testing ("DAST"), that are used for good faith cybersecurity research strips a leg of protection from the already limited methods of proactive security. Instead, government agencies and lawmakers need to become more aware of the vast benefits of true cybersecurity research and the tools and methods needed to conduct such research for the greater good. This awareness will ultimately lead to cyber defense enablement and the elimination of antiquated laws, sometimes preventing or hindering effective cyber research.

III. DIGITAL MILLENNIUM COPYRIGHT ACT

The DMCA is a unique regulatory mechanism created by the U.S. copyright system.[72] Taken in scope with the constitutional directive of the Copyright Clause[73], as well as the fair use doctrine[74] codified in Section 107 of the Copyright Act[75], the DMCA attempts to balance the competing interest of copyright holders and the public at large. In other words, the DCMA attempts to protect content creators while balancing the content users' (i.e., researchers, consumers, etc.) freedom of ownership after purchasing copyrighted material.

A. History of the DMCA

The foundation of the DMCA centered around the United States' commitment to observe two treaties passed by the WIPO in December 1996. During the Berne Convention, held at the WIPO headquarters, two treaties—dedicated to updating international copyright laws—were designed.[76] The two treaties dealt with copyright's involvement with modern information systems like the Internet.[77] The

72. Maryna Koberidze, *The DMCA Rulemaking Mechanism: Fail or Safe?*, 11 WASH. J.L. TECH. & ARTS 211 (2015), available at https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1235&context=wjlta [https://perma.cc/8G5R-G6AJ] (Noting that Australia is the only other country in the world that has similar rulemaking provisions. Additionally, the adoption of such a procedure was to comply with the terms of the Free Trade Agreement); *See The Australia-United States Free Trade Agreement*, art. 17.4, ¶ 7, OFFICE OF THE U.S. TRADE REPRESENTATIVE (eff. Jan. 1, 2005), available at https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file469_5141.pdf [https://perma.cc/END5-XUZ9].

73. U.S. CONST. art. I, § 8, cl. 8 ("The Congress shall have power . . . [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their [] Writings and Discoveries.").

74. *Copyright and Fair Use*, OFFICE OF THE GENERAL COUNSEL (Feb. 16, 2023), https://ogc.harvard.edu/pages/copyright-and-fair-use [https://perma.cc/B8UD-A9ZN] (defining fair use as "the right to use a copyrighted work under certain conditions without permission of the copyright owner.").

75. 17 U.S.C. § 107 (1976), amended by Pub. L. No. 102-492, 106 Stat. 3145 (allowing fair uses of copyrighted material, including for purposes of criticism, comment, news reporting, teaching, scholarship, or research, etc.).

76. Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121 (2006).

77. *WIPO Copyright Treaty (WCT)*, WORLD INTELLECTUAL PROPERTY ORGANIZATION https://www.wipo.int/treaties/en/ip/wct/ [https://perma.cc/SLY3-7TVL] (summarizing the WIPO as "a special agreement under the Berne Convention which deals with the protection of works and the rights of

United States, as a member of WIPO, was required to implement similar copyright protections.[78] Congress, in its efforts to "begin updating national laws for the digital era,"[79] arranged the DMCA to "facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.'"[80] Therefore, expanding intellectual property protections for copyright holders was paramount to survival in the digital age. The DMCA was the United States' way of conforming to the demands of the WIPO.[81]

The purpose of copyright law is to protect and maintain original works of authorship.[82] With the progression of the digital age, the DMCA lends a hand in safeguarding digital media from malicious actors.[83] Initially, the Library of Congress had complete autonomy over copyrighted material. Later, however, the Library of Congress added the Copyright Office to its agency. Because of this, the Office is now the leading body on copyright issues and "operates by working with copyright owners who are in the process of registering their works, while also reviewing former registered works."[84] The Office remains a branch of the Library of Congress and "administers the national copyright system and provides advice on copyright law to congress, federal agencies, the courts and the public."[85]

The Office must consider comments, policy proposals, and copyright law and legislation exemptions every three years.[86] Congress is advised "on copyright law changes," and "the Copyright Officer references proposals and comments received

---

their authors in the digital environment." Moreover, the WIPO Copyright Treaty also is concerned with two subject matters to be protected by copyright: (i) computer programs, no matter the mode or form of their expression; and (ii) databases, which is the compilations of data or other material).

78. *Id*.

79. H.R. Rep. No. 105-551, pt. 2, at 21 (1998). The objective of Title I of the DMCA was to revise U.S. copyright law to comply with two recent WIPO treaties and to strengthen copyright protection for motion pictures, sound recordings, computer software and other copyrighted works in electronic formats.

80. *Joint Study of Section 1201(g) of The Digital Millennium Copyright Act*, U.S. COPYRIGHT OFFICE https://www.copyright.gov/reports/studies/dmca_report.html (citing S. Rep. No. 105-190, at 1 (1998)) [https://perma.cc/4CCH-9DRQ].

81. *Digital Millennium Copyright Act*, AMERICAN LIBRARY ASSOCIATION (Jan. 24, 2019), http://www.ala.org/advocacy/copyright/dmca [https://perma.cc/QP36-EH4L].

82. Weigle, *supra* note 12, at 11–12 (citing 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)).

83. *See* 17 U.S.C. § 1201 (2012).

84. Weigle, *supra* note 12, at 11.

85. *Copyright Office*, USA.GOV, https://www.usa.gov/federal-agencies/copyright-office [https://perma.cc/2CSS-7QZF].

86. *Overview of the Copyright Office*, COPYRIGHT OFFICE (December 2016) https://www.copyright.gov/about/. There is limited guidance regarding the rulemaking process of the of the DMCA. Section 1201(a)(1)(C) provides that it is to be "conducted by the Register (who is also the Director of the Copyright Office)[] and overseen by the Librarian." Koberidze, *supra* note 72, at n. 93 ("It is no coincidence that Congress entrusted the Register to aid the Librarian in the rulemaking proceeding. Since its creation in 1897, the Copyright Office, as a part of the Library of Congress, has proven to be a tremendous asset to Congress itself. 17 U.S.C. § 1201(a)(1)(C) (2000)"); 17 U.S.C. § 1201(a)(1)(C)–(B) (2000). There is no instruction over how the Office must conduct its proceedings, nor is there any useful guidance as to the weight that must be provided to the opinions of the NTIA's Assistance Secretary. Koberidze, *supra* note 72 at n. 88 (citing H.R. REP. NO. 105– 796, at 64 (1998) (stating that "[t]he determination [of affected classes of works] will be made in a rulemaking proceeding on the record")). Notably, the DMCA has yet to define "'a particular class of copyrighted works,' as to which the exemptions to be considered by the Register and the Librarian, or provided the standard of harm to justify" these exemptions. *Id*. at 234 – 35 (citing 17 U.S.C. § 1201(a)(1)(C)–(B)).

from scholars, agencies, and corporations."[87] After the Office gives Congress suggestions about copyright law changes, Congress decides whether to amend or adopt these changes. In its most recent consideration, in 2021, the Office focused narrowly on the exemptions to prohibition on circumvention of copyright protection systems for access control technologies under Section 1201 of the DMCA.

B. Development of Section 1201

The technological developments that have come to pass—due to the digital age—shifted the Office from its original goal of "registering and serving as a copyright records office, to regulating copyright use through implement[ing]…laws, such as the DMCA."[88] Initially, Congress passed the DMCA to accomplish three main goals: (i) protect copyright holders, (ii) protect internet service providers, and (iii) protect specific internet platforms from users' copyright violations. Unfortunately, although the DMCA benefits copyright holders, it limits the freedom of those who purchase copyrighted materials and risks making certain types of security research a violation of copyright law.[89]

The DMCA covers various topics, from Fair Use exemptions to the recent provisions prohibiting the circumvention of TPMs on computer programs for good-faith security research.[90] For example, the exemption for good-faith security research allows a security researcher to circumvent technology software if the circumvention qualifies as 'good faith security research.' The new rules provide that "good-faith security research" means:

> accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, 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, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.[91]

The new rules to the DMCA are a much-needed step forward for providing greater legal protections for independent security researchers. The recent amendments will hopefully mitigate cybercrime by creating a more robust outlook on security research and "allow[] researchers the opportunity to discover security vulnerabilities through the circumvention of targeted software."[92] This also allows

87. Weigle, *supra* note 12, at 11; *See U.S. Copyright Office*, POLICY REPORTS, 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).

88. Weigle, *supra* note 12, at 12 (citing 17 USC § 1201).

89. Meysenburg, *supra* note 69.

90. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R § 201 (2021) (discussing the DMCA's exemptions surrounding anti-circumvention by security researchers).

91. *Id*.

92. Weigle, *supra* note 12 (citing Copyright Act of 1976, 17 U.S.C. § 102 (2012)).

companies to mitigate or remediate internet-accessible systems and services vulnerabilities or vendors' internet-accessible systems or services.

Section 1201 prohibits the circumvention of "a technological measure that effectively controls access to a work."[93] TPMs take many forms, such as Digital Rights Management ("DRM"). DRM is a method of limitation used by copyright holders to restrict how digital files are used.[94] For example, if you purchase an eBook "but are prevented from copying it from your [eBook] reader to your phone, that is likely DRM at work."[95] Additionally, regarding the anti-circumvention prohibition, Section 1201 stops distribution tools used to upset TPMs (i.e., anti-trafficking provisions).[96]

Generally, the prohibitions against upsetting TPMs suggest a focus on protecting content from digital piracy (such as copy protection on music devices). Still, the DMCA covers other copyrighted digital works, such as computer codes. Moreover, Section 1201's definition of "circumvent a technological measure" is relatively broad as it includes anyone who may, among other things, "avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[97] This definition makes security researchers question whether they are in an area of legal permissibility.

As opposed to the Computer Fraud and Abuse Act of 1986 ("CFAA")[98], the DMCA recognizes the need to provide "reasonable exemptions to Section 1201's anti-circumvention prohibitions."[99] Within Section 1201, there are several permanent exemptions for security testing and encryption research.[100] Importantly, however, the DMCA imposes specific requirements to qualify for these

93. 17 USC § 1201.

94. Meysenburg, *supra* note 69.

95. *Id*.

96. *Id*.; *see* Christen da Costa, *What Are DMCA Exemptions*, SECTION 1201 EXEMPTIONS TO PROHIBITION OVERVIEW (Oct. 26, 2022), https://www.gadgetreview.com/what-is-dmca-exemptions [https://perma.cc/VY8W-ZYLZ] (providing that "TPMs are defined under the law as anything that grants access to an otherwise copyright-protected work").

97. 17 USC § 1201 (a) (3) (A); In re Dealer Mgmt. Sys. Antitrust Litig., 581 F. Supp. 3d 1029, 1096 (N.D. Ill. 2022) (Providing that when defining "circumvention" of a technological access measure, "experts may provide opinions as to the ultimate factual issues in a case," however, experts may not testify as to the legal conclusions used in determining the result of the case under the Federal Rules of Evidence 702. Here, the expert witness attempted to go beyond the scope of her privileges by "qualify[ing] the impact" of the wrongdoing. Nevertheless, the court stated that the "testimony on common practices in the industry would be a piece of [plaintiff's] larger defense"); *see* Yout, LLC v. Recording Indus. Ass'n of Am., Inc., No. 3:20-cv-1602 (SRU), 2022 U.S. Dist. LEXIS 178462, at *43-44 (D. Conn. Sep. 30, 2022) (stating that courts have held that a wide range of technological measures that are not expressly incorporated in Section 1201 are "'effective,' including password protection and validation keys); *E.g.,* Adobe Sys. v. Feather, 895 F. Supp. 2d 297, 302 (D. Conn. 2012) (activation and validation keys for software).

98. Stan Adams, *The Supreme Court and the Copyright Office Have an Important Opportunity to Shore Up Much-Needed Security Research*, CENTER FOR DEMOCRACY AND TECHNOLOGY (July 9, 2020), https://cdt.org/insights/the-supreme-court-and-the-copyright-office-have-an-important-opportunity-to-shore-up-much-needed-security-research/ [https://perma.cc/AY9F-6ACG] (summarizing the CFAA as a design meant "to prevent malicious actors from accessing government-controlled computers); *see* Computer Fraud and Abuse Act of 1986, PUB. L. NO. 99–474, 100 Stat. 1213, https://www.congress.gov/bill/99th-congress/house-bill/4718/text [https://perma.cc/4QYN-E8NC] (creating new Federal criminal offenses of: (1) property theft by computer occurring as part of a scheme to defraud; (2) altering, damaging, or destroying information in, or preventing the authorized use of, a Federal interest computer; and (3) trafficking in computer access passwords).

99. Meysenburg, *supra* note 69.

100. *Id*.

exemptions—based on the CFAA's broad definition of exceeding authorized access.[101] In addition to the qualifying factors, researchers must prove that the code they use for their research is not "primarily designed or produced for the purpose of circumventing a technological measure," thus infringing on the anti-trafficking provision.[102] Although these rules are not set in stone, the Office is strongly recommended to modify its current administrative procedures to the rulemaking process.[103] The Register of Copyrights and the Librarian of Congress should revisit the three-year interim between hearings (regarding the response to a public request and comment process) because it leaves too much room for error.

On October 26, 2018, based on the Acting Register of Copyrights recommendation, the Librarian of Congress adopted exemptions to Section 1201—prohibiting circumvention of technological measures that control access to copyrighted works.[104] The exemptions are determined by the Librarian of Congress, from the recommendation of the Register of Copyright, and— as stated above— are in effect for three years.[105] Significant ambiguities that could cause "researchers to avoid publicly beneficial research activities" were the topic of discussion during the seventh triennial rulemaking proceeding.[106] Those suggested (and crucial) changes were to a good-faith security research exemption, broadening security researchers' ability to lawfully test device and system software for cybersecurity vulnerabilities without violating the DMCA and risking criminal liability.[107] Proponents argued that those limitations adversely affect researchers from good-faith, fair use investigations into device and system software security.[108]

The proponents argued that exemptions to "Device Limitation" (i.e., limiting the exemption to consumer devices) interfered with researchers' ability to

101. *Id*.; *see also* Aaron Burstein, *A Survey of Cybercrime in the United States*, 18 Berk. T. L.J. 313, 331 (2003) (providing that the CFAA has been under "strong criticism [for its] failure to define 'access' render[ing] it incoherent and broader than intended").

102. *See* 17 U.S.C. § 1201(a)(2)(A).

103. *See* Maryna Koberidze, *supra* note 72, at 215–17 (stating that

> Critics of the process claim it is: Unduly burdensome — especially for proponents seeking renewals of prior exemptions, who are required to demonstrate actual or probable substantial harm to non-infringing uses of copyrighted works in every rulemaking; Repetitive — specifically, due to the de novo standard of review that applies equally to petitions requesting new exemptions and those requesting renewals of the existing ones; Too narrow — generally, only few exemptions are granted upon each rulemaking, and those granted are usually limited to a narrow class of works, do not extend to circumvention tools, and sometimes last even less than three years; Too long — typically, a rulemaking proceeding takes about one year to conclude, with exception for the 2010 Rulemaking that lasted almost twenty months; and Overly complex — which makes the process less comprehensible for the general public and often forces its participants to engage attorneys, thus making it quite costly).

104. *Section 1201 Security Research Exemption*, SAMUELSON-GLUSHKO TECHNOLOGY LAW & POLICY CLINIC (TLPC), (Nov. 20, 2018), https://tlpc.colorado.edu/section-1201-security-research-exemption/.

105. 17 U.S.C. § 1201(a)(1)(C) (This review is a fail-safe for Congress allowing them to enforce circumvention prohibitions or grant them every three years. If a law is deemed unfavorable after three years, Congress retains the options to review and amend the law. Section 1201's permanent exemptions, including Section 1201(d) establishing an exemption, under specific circumstances, for nonprofit libraries, archives, or educational institutions to circumvent technological measures to make a good faith determination of whether to acquire a copy of the work).

106. *Rulemaking Proceedings Under Section 1201 of Title 17*, U.S. COPYRIGHT OFFICE https://cdn.loc.gov/copyright/1201/; *see* Arielle Singh, *Agency Regulation in Copyright Law: Rulemaking Under the DMCA and Its Broader Implications*, 26 BERKLEY TECH. L.J. 527-28 (2011).

107. *Section 1201 Security Research Exemption*, *supra* note 104.

108. *Id*.

investigate larger systems such as "building automation systems, avionics, traffic control infrastructure, or voting machines."[109] Additionally, proponents argued against the limitation on performing security research in "controlled environments," which suggests the exemption had limited 'research' to "a lab-like setting."[110] Finally, proponents argued against the narrow circumvention exemption for software security research that is contingent on researchers not violating any applicable law,[111] including the CFAA.[112] Ultimately, the Acting Register of Copyrights found equitable claims in some of these arguments and recommended that "Device Limitation" be eliminated and "Controlled Environment" be narrowed.[113] The Librarian of Congress adopted the recommendations, applying the exemption to research conducted on all "computer programs" located on devices lawfully acquired or on systems whose operators have given authorization.[114] In addition, the "controlled environment" exemption was narrowed to an "environment designed to avoid any harm to individuals or the public."[115] Although, the Acting Register was not persuaded by the argument requiring security researchers to follow all "applicable laws," so it remained in the 2018 exemptions.[116] Nevertheless, in 2021, the Acting Register agreed the limitations were "'likely to impose an adverse effect on noninfringing security research.'"[117] The Register noted, however, that this exemption does not allow one to waive liability under "'other laws while performing good-faith security research.'"[118]

In October 2021, the Office again updated its exceptions for security research. "No oppositions were filed against readoption of [the circumvention exemption for good-faith security research], and Consumer Reports submitted a comment in support of the renewal petition."[119] Proponents demonstrated a need for the continued exemption:

> For example, Professor J. Alex Halderman, the Center for Democracy and Technology . . . , and the U.S. Technology Policy Committee of the Association for Computing Machinery . . . highlighted the need to find and detect vulnerabilities in voting machines and other election systems, the increased proliferation of consumer Internet of Things devices, and the

109. *Id*.

110. *See e.g.*, *Section 1201 2018: Frequently Asked Questions*, U.S. COPYRIGHT OFFICE, https://www.copyright.gov/1201/2018/faqs.html [https://perma.cc/EK4W-KX6C] (last visited Jan. 4, 2023).

111. *See* 37 C.F.R § 201.40(b) (5)(ii)(11) (existing exemption for good-faith security research).

112. *Section 1201 2018: Frequently Asked Questions*, *supra* note 110; *see Section 1201 Security Research Exemption*, *supra* note 104.

113. Evelyn Remaley, *Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, Docket No. 2020–11*, (Oct. 21, 2021), https://cdn.loc.gov/copyright/1201/2021/2021_NTIA_DMCA_Letter.pdf.

114. SAMUELSON-GLUSHKO TECHNOLOGY LAW & POLICY CLINIC (TLPC), *supra* note 104.

115. *Id*.

116. *Id*.

117. Meysenburg, *supra* note 69.

118. *Id.*

119. Recommendation of the Register of Copyrights, *Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention*, U.S. COPYRIGHT OFFICE, at 27 (Oct. 2021) (citing Consumer Reports Security Research Comment; citing Campos Medical Devices Renewal Pet. at 4 ("[W]e also support the petition for an exemption for good-faith security research, which is critical to ensure our medical devices are secure from vulnerabilities.")).

> increasing reliance on digital systems combined with greater aggressiveness on the part of threat actors, including other nation states. [Additionally,] in the past three years, ". . . [there have been] threats of litigation from copyright holders in connection with his security research on software in voting systems." Finally, MEMA stated that its membership "experienced firsthand that the exemption is helping encourage innovation in the automotive industry while mitigating risks to intellectual property and vehicle safety," and opined that the current exemption strikes an "appropriate balance."[120]

Rules, laws, and regulations will never be able to keep up with technological changes. That, however, does not mean appropriate committees cannot make predictions and forecast technological advancements—taking proactive, as opposed to reactive, steps to evolve the law. A vital consideration should therefore be given to the Office's effectiveness. As opposed to approaching security issues with an eye toward the future, the Office contemplates past harms that have already progressed through their adolescence before taking corrective measures. The Office and the Library of Congress should acknowledge the expertise of groups and organizations who advocate for less restrictive provisions of DMCA. While arguments can be made that the DMCA seeks to protect the rights of copyrighted work, the DMCA does not promote growth, nor does it develop an efficient electronic marketplace.

IV. NOTABLE INSTANCES OF THE "WORST" CRIMINAL CHARGES AGAINST SECURITY RESEARCHERS

Section 1201 of the DMCA is criticized for being overbroad and stifling innovation, creativity, and free speech. As such, several instances illustrate Section 1201 being applied in a way deemed unfair and disproportionate—especially in software security research and anti-circumvention of DRM systems.[121] Although it

120. Recommendation of the Register of Copyrights, *supra* note 119, at 28.

121. *See, e.g.*, Timothy Geigner, *Mystery Over Fake Section 1201 Takedown Claims Sent By 'Video Industry Association of America' Deepens*, TECHDIRT (Sept. 3, 2021, 7:39 PM), https://www.techdirt.com/2021/09/03/mystery-over-fake-section-1201-takedown-claims-sent-video-industry-association-america-deepens/ [https://perma.cc/LUX9-DEDV] (Fake Section 1201 takedown claims refer to false or fraudulent assertions made under the guise of the DMCA that a particular activity constitutes circumvention of TPMs, as prohibited by Section 1201 of the DMCA. These fake takedown claims are often meant to harass or silence people engaging in lawful activities, like reverse engineering or security research, or suppress competition in markets for repair and compatibility services. The use of fake Section 1201 takedown claims can have severe consequences for the individuals and organizations targeted by these claims. For example, it can result in removing lawful content from websites or censoring lawful speech. Additionally, the recipient of a false takedown claim may face significant legal expenses to challenge the claim's validity. To address this problem, some have called for greater transparency and accountability in the DMCA takedown process and for adopting measures to protect free speech and innovation from the abuse of TPMs and anti-circumvention laws like the DMCA); *see also* Ernesto Van der Sar, *'Fraudulent' DMCA Circumvention Takedowns Target Prominent Websites*, TORRENTFREAK (Sept. 2, 2021), https://torrentfreak.com/fraudulent-dmca-circumvention-takedowns-target-prominent-websites-210902/ [https://perma.cc/W7EZ-UCDX]. (Section 1201 has facilitated the notice of abuse by bad-faith parties:

> "A mysterious group called the 'Video Industry Association of America' is trying to wipe the homepages of dozens of reputable sites from Google search. The targets, which stand accused of violating the DMCA's anti-circumvention policy, include Verizon, Pinterest, and Engadget. Google says that it's aware of these fraudulent notices but, thus far, they are not without damage. . . . The 'American' organization starts one request off in Russian and finds it hard to construct proper English sentences. In another notice, it complains of sites and apps that circumvent the copyright protection of streaming services, while classifying these as "software

is difficult to discern the "worst" criminal charges against security researchers under Section 1201 of the DMCA—likely as the consequences of violating the provisions of the law can vary greatly depending on the circumstances of each case.[122]

A couple of notable cases that have generated significant public attention and controversy include the following: (1) Dmitry Sklyarov, a Russian programmer who was arrested and charged with violating the DMCA in 2001 for his work on a software program that allowed users to bypass Adobe Systems' eBook security measures.[123] The charges against Sklyarov were eventually dropped, but the case drew attention to the impact of the law on security research and the potential consequences of violating the provisions of the DMCA. (2) Marcus Hutchins, a British security researcher, was arrested and charged with six counts of violating the DMCA in 2017 for his work on the Kronos banking Trojan.[124] Hutchins was eventually sentenced to time served, but the case highlights the potential consequences of violating the provisions of the law, even when the researcher intended to improve computer security.

A. *United States v. Elcom Ltd.*

Dmitry Sklyarov ("Sklyarov") was a Russian programmer embroiled in a high-profile case related to Section 1201 of the DMCA in 2001. Sklyarov was charged with violating the DMCA for his work on a software program that allowed users to bypass Adobe Systems' eBook security measures.[125] The case raised important questions about the impact of the law on security research and the potential consequences of violating the provisions of the DMCA. Sklyarov worked for the Russian software company Elcomsoft, which developed a program called Advanced eBook Processor.[126] The software allowed users to remove the encryption from Adobe's eBooks, making it possible to read the books on different devices and platforms.[127] Adobe claimed that this was a violation of its copyright, and that the software was illegal under the provisions of the DMCA.[128]

In July 2001, Sklyarov was arrested while in the United States to give a presentation about his work at the DEFCON conference in Las Vegas.[129] He was charged with five counts of violation of the DMCA and faced the prospect of

cracks." Things get even more problematic when we look at the URLs that are reported. While these include tools such as DVDFab and YouTube-rippers, which some rightsholders see as problematic, various legitimate sites are targeted as well.")

122. *See, e.g.*, Mike Masnick, *Bill Introduced To Fix Broken DMCA Anti-Circumvention Rules*, TECHDIRT (Apr. 17, 2015, 6:24 PM), https://www.techdirt.com/2015/04/17/bill-introduced-to-fix-broken-dmca-anti-circumvention-rules/ [https://perma.cc/FLK7-C8Z8].

123. *See* Out-Law News, *Charges dropped against Dmitry Sklyarov*, PINSENT MASONS (Dec. 14, 2001, 12:00 AM), https://www.pinsentmasons.com/out-law/news/charges-dropped-against-dmitry-sklyarov [https://perma.cc/UB3A-X7MZ].

124. *See* Michael Heller, *Marcus 'MalwareTech' Hutchins pleads guilty to Kronos charges*, TECHTARGET (Apr. 22, 2019), https://www.techtarget.com/searchsecurity/news/252462053/Marcus-MalwareTech-Hutchins-pleads-guilty-to-Kronos-charges [https://perma.cc/VR5Y-FW9J].

125. *See United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1118 (N.D. Cal. 2002).

126. *See id*.

127. *Id*.

128. *See id.* at 1119.

129. *Russian hacker arrested after Las Vegas convention*, THE GLOBE AND MAIL (July 18, 2001), https://www.theglobeandmail.com/technology/russian-hacker-arrested-after-las-vegas-convention/article1184011/ [https://perma.cc/ZS4F-T9AU].

spending years in prison if convicted.[130] The arrest and prosecution of Sklyarov were seen as a test case for the provisions of the DMCA and the extent to which they would be enforced.[131] The federal prosecutors eventually permitted Sklyarov to return home, but brought criminal charges against ElcomSoft.[132] The court held that the DMCA would not permit copyright owners to prohibit eBooks going into the public domain and stated:

> Upon the expiration of the copyright, there is no longer any protectable intellectual property right in the work's expression. The expression may be copied, quoted, republished in new format and sold, without any legally enforceable restriction on the use of the expression. The publisher/copyright owner has no right to prevent any user from using the work any way the user prefers. At best, the publisher has a technological measure embedded within the digital product precluding certain uses of that particular copy of the work and, in many cases, the user/purchaser has acquiesced in this restriction when purchasing/licensing the work. *See* End User License Agreements, O'Connell Decl. Exhs. A-D. The essence of a copyright is the legally enforceable exclusive rights to reproduce and distribute copies of an original work of authorship, to make derivative works, and to perform the work publicly, for a limited period of time. 17 U.S.C. §§ 106, 302-303. None of those rights is extended beyond the statutory term merely by prohibiting the trafficking in or marketing of devices primarily designed to circumvent use restrictions on works in electronic form.[133]

Importantly, this case had broader implications for the security research community and the technology industry. It highlighted the potential legal repercussions researchers face regarding their work and the limitations of existing laws in protecting security research.[134] Security researchers around the globe saw the lawsuit as evidence of a growing trend of criminalizing security research, which could have a chilling effect on the field and make it more challenging for researchers to identify and fix vulnerabilities in software and hardware systems.[135]

Ultimately, charges against Sklyarov were dropped, but the case had already drawn attention to the impact of the DMCA on security research. Additionally, the incident led to widespread criticism of the law and calls for reform.[136] It also contributed to the growing debate about the role of the government and the technology industry in regulating online behavior. *United States v. Elcom Ltd.* highlights the potential consequences of violating the provisions of the DMCA and

130. *US v. ElcomSoft & Sklyarov FAQ*, ELECTRONIC FRONTIER FOUNDATION (Apr. 21, 2008), https://www.eff.org/pages/us-v-elcomsoft-sklyarov-faq [https://perma.cc/YB2B-YSXD].

131. *See Id*.

132. *US v. ElcomSoft & Sklyarov FAQ*, *supra* note 130.

133. *Elcom Ltd.*, 203 F. Supp. 2d at 1141.

134. *See* Lisa M. Bowman, *ElcomSoft verdict: Not guilty*, ZDNET (Dec. 17, 2002), https://www.zdnet.com/article/elcomsoft-verdict-not-guilty/.

135. Nat Meysenburg, *Cybersecurity Research Should Not Be A Crime: Why We Need Clear, Permanent CFAA and DMCA Exemptions*, NEW AMERICA. (Nov. 18, 2021), https://www.newamerica.org/oti/briefs/cybersecurity-research-should-not-be-a-crime/ [https://perma.cc/R29N-RLE2].

136. *See generally* Stephanie Ardito, *The Case of Dmitry Sklyarov*, INFORMATIONTODAY https://www.infotoday.com/it/nov01/ardito.htm [https://perma.cc/QV9S-777E].

the need for greater legal protections for security researchers.[137] Furthermore, the incident serves as a reminder of the importance of balancing the interests of copyright owners with the need to promote security research and the free flow of information.

B. The Kill Switch Discovery

Marcus Hutchins ("Hutchins"), also known by his online handle "MalwareTech,"[138] is a British security researcher who was embroiled in a high-profile case following a ransomware attack shutting down a dozen United Kingdom hospitals.[139] Hutchins was arrested and charged with six counts of violating the provisions of the law for his work on the Kronos banking Trojan.[140] The case raises important questions about the impact of the law on security research and the potential consequences of impeding on good faith hackers.[141]

Hutchins rose to prominence in the security community in 2017 when he discovered a kill switch for the WannaCry ransomware attack, which caused global widespread disruption.[142] "WannaCry is less of a threat in large part, thanks to the heroics of Marcus Hutchins. The British computer security researcher developed a kill switch using reverse engineering and honeypots, preventing WannaCry from executing further. In addition, a team of French researchers found a way to decrypt some affected computers without paying a ransom."[143] However, later that year, Hutchins was arrested in the United States for his work on the Kronos banking Trojan, allegedly used to steal financial information from victims.[144] Hutchins, in 2019, pleaded guilty to "one count of conspiracy to commit computer fraud in

137. *Unintended Consequences: Ten Years under the DMCA*, ELECTRONIC FRONTIER FOUNDATION (Oct. 27, 2008), https://www.eff.org/wp/unintended-consequences-ten-years-under-the-dmca [https://perma.cc/KQZ4-9YNC].

138. Joseph Cox, *Researcher Who Stopped WannaCry Ransomware Detained in US After Def Con*, MOTHERBOARD (Aug. 3, 2017), https://www.vice.com/en/article/ywp8k5/researcher-who-stopped-wannacry-ransomware-detained-in-us-after-def-con [https://perma.cc/N74Y-WZD9]; *see also WannaCry Ransom Notice Analysis Suggests Chinese Link*, BBC NEWS (May 29, 2017), http://www.bbc.com/news/technology-40085241 [https://perma.cc/DNM9-URUR]; *see What was WannaCry? |WannaCry Ransomware*, MALWAREBYTES, https://www.malwarebytes.com/wannacry [https://perma.cc/2CVR-A7PX]; *see* Danny Palmer, *China on WannaCry: It Wasn't Us, Honest*, ZDNET (Jun 13, 2017), http://www.zdnet.com/article/china-on-wannacry-it-wasnt-us-honest/ [https://perma.cc/324H-XVPU].

139. Cox, *supra* note 138.

140. *Id*.; United States v. Hutchins, 361 F. Supp. 3d 779, 786 (E.D. Wis. 2019); *see generally Marcus Hutchins 'Saved the U.S.' from WannaCry Cyberattack on Bedroom Computer*, NBC NEWS (May 16, 2017, 8:18 AM ET), https://www.nbcnews.com/storyline/hacking-of-america/marcus-hutchins-saved-u-s-wannacry-cyberattack-bedroom-compter-n759931 [https://perma.cc/JLT4-EQS3].

141. K. K. e Silva, *Vigilantism and Cooperative Criminal Justice: Is There a Place for Cybersecurity Vigilantes in Cybercrime Fighting?*, 32 INT. REV. L. COMPUTERS & TECH. 27 – 29 (2018).

142. *Marcus Hutchins 'Saved the U.S.' from WannaCry Cyberattack on Bedroom Computer*, *supra* note 140; Andrew Moshirnia, *No Security Through Obscurity: Changing Circumvention Law to Protect our Democracy Against Cyberattacks*, 83 BROOKLYN L. REV. 1279, 1332 (2018).

143. *What was WannaCry? |WannaCry Ransomware*, Malwarebytes, https://www.malwarebytes.com/wannacry [https://perma.cc/S63W-7BBW].

144. Leila Fadel, *Feds Arrest Man Credited With Helping To Stop Ransomware Attack*, NPR (Aug. 3, 2017), https://www.npr.org/sections/thetwo-way/2017/08/03/541447479/feds-arrest-man-credited-with-helping-to-stop-ransomware-attack [https://perma.cc/MGA3-9C3S].

violation of Title 18" and "one court of advertising a devised used to intercept electronic communications."[145]

The case of Marcus Hutchins emphasizes the potential consequences of violating the provisions of the CFAA, even when the researcher intended to improve computer security.[146] Many security researchers saw the case as evidence of a growing trend of criminalizing security research, which could have a chilling effect on the field and make it harder for researchers to identify and fix vulnerabilities in software and hardware systems.[147] Importantly, "lawyers and researchers following the case," say that the issue "is not a matter of Hutchins's guilt or innocence. Rather, it's the rollout of an indictment they say is short on facts, was aggressive in its application of computer law[,] and ultimately left researchers confused over whether standard research practices are now being treated as prosecutable offenses."[148]

The arrest and prosecution of Hutchins also raised questions about the applicability of the current legislation to good faith security research.[149] Deputy Attorney General Lisa Monaco stated that the DOJ "'has never been interested in prosecuting good-faith [ ] security research.'"[150] As such, Hutchins demonstrates the need for greater legal protections for security researchers.[151] In the end, Hutchins was sentenced to time served and returned to the United Kingdom.[152] However, the case had already drawn attention to the impact security research has on the safety of

145. *Marcus Hutchins Pleads Guilty to Creating and Distributing the Kronos Banking Trojan and UPAS Kit Malware*, (May 3, 2019), https://www.justice.gov/usao-edwi/pr/marcus-hutchins-pleads-guilty-creating-and-distributing-kronos-banking-trojan-and-upas [https://perma.cc/45TK-H8LX].

146. Marcelo Triana, *Note: Is Selling Malware a Federal Crime?*, 93 N.Y.U.L. Rev. 1313 (2018); *see* Karen Epper Hoffman, *A Black and White Issue?*, SC MEDIA (Nov. 7, 2016), https://www.scmagazine.com/a-black-and-white-issue/article/571260/ [https://perma.cc/DQ85-TRS4].

147. Triana, *supra* note 146.

148. Joe Uchill, *Arrest of WannaCry researcher sends chill through security community*, THE HILL (Aug. 4, 2017, 1:17 pm), https://thehill.com/policy/cybersecurity/345337-wannacry-hero-chills-security-community/ [https://perma.cc/4MR7-C5LG] (Many experts argue that the arrest and prosecution of Hutchins sends a chilling message to others in the cybersecurity community and could discourage them from reporting vulnerabilities to companies and government agencies. This is evident in a statement by Jake Williams, the founder of Rendition Infosec, which had been tracking the WannaCry ransomware worm's use of recently patched exploit stolen from the NSA. Mr. Williams stated that "[Rendition Infosec] did a lot of work on WannaCry, too . . . I had folks afraid that their own involvement in investigating WannaCry would get them arrested").

149. K. K. e Silva, *supra* note 141, at 28 (arguing that "Hutchins did not infringe on any specific legislation, in that his response to the malware was as simple as registering the domain hardcoded in Wannacry"); Andy Greenberg, *The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet*, WIRED (May 12, 2020), https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/ [https://perma.cc/3Z4F-USFT].

150. *What Counts as "Good Faith Security Research?"*, KREBSONSECURITY (June 3, 2022), https://krebsonsecurity.com/2022/06/what-counts-as-good-faith-security-research/ [https://perma.cc/24PE-AD3B].

151. Riana Pfefferkorn, *The Importance of Protecting Good-faith Security Research*, THE CENTER FOR INTERNET AND SOCIETY (Sept. 14, 2020, 9:38 am), https://cyberlaw.stanford.edu/blog/2020/09/importance-protecting-good-faith-security-research [https://perma.cc/UKF5-3EJJ].

152. Bruce Vielmetti & Keith Schubert, *WannaCry virus hero Marcus Hutchins is spared prison time for his earlier malware exploits*, MILWALKEE JOUNRAL SENTENIAL (July 26, 2019), https://www.jsonline.com/story/news/crime/2019/07/26/wannacry-virus-hero-marcus-hutchins-spared-prison-earlier-malware/1826012001/ [https://perma.cc/V2H8-7E6J].

hundreds of thousands of people worldwide.[153] In addition, it contributed to the growing debate about the role of the government and the technology industry in regulating online behavior.[154]

The heroic act of Marcus Hutchins highlights the need for greater legal protections for security researchers and the importance of promoting security research and the free flow of information.[155] In addition, the incident serves as a reminder of the potential consequences of violating the provisions of laws like the CFAA and the importance of understanding the limitations of existing laws in protecting security research. Prosecuting researchers for their work can therefore stifle innovation. Cybersecurity innovation often comes from security researchers discovering vulnerabilities and creating tools to address them, like the kill switch.[156] As such, prosecuting researchers for their work can stifle innovation and make it more challenging to address cybersecurity threats.[157] As the EFF notes, "[a]s we increasingly move our public debate from traditional media to online outlets, the security of this environment becomes essential for the protection of our most fundamental human rights: freedom of expression, freedom of association, and privacy."[158]

V. REACTION TO GROWTH: CFAA VS. DMCA

The DMCA is a dangerous law that threatens cybersecurity, speech, and competition.[159] Although the DMCA has made strides in loosening its grip on some exemptions, the law is still too broad and is not conducive to digital development in law or otherwise.[160] Moreover, copyright, generally, "is not an absolute legal

153. Greenberg, *supra* note 149; *see* Zack Whittaker, *Malware researcher Marcus Hutchins pleads guilty, ending his legal case*, TECHCRUNCH+ (Apr. 19, 2019), https://techcrunch.com/2019/04/19/malwaretech-legal-case-over/ [https://perma.cc/6LV2-L62J].

154. Tyler Campbell, *The Moral Code of Marcus Hutchins, a Hacker Who Saved the Internet*, INFORMATION SECURITY – A SHARED RESPONSIBILITY, (June 8, 2020), https://infosec.conncoll.edu/uncategorized/the-story-of-marcus-hutchins-a-hacker-who-saved-the-world/ [https://perma.cc/4CQ9-9LDL] (stating that the judge "who had been assigned to Marcus's case . . . recognized that Marcus would be a valuable asset in protecting society from future malicious cyber attacks").

155. Elizabeth Weise, *His life got weird after saving the Internet: ransomware hero Marcus Hutchins*, USATODAY.COM (May 23, 2017), https://www.usatoday.com/story/tech/talkingtech/2017/05/23/ransomware-hero-marcus-hutchins-says-tabloids-invaded/102026238/ [https://perma.cc/BYW7-V5PZ].

156. Andy Greenberg, *The WannaCry Ransomware Hackers Made Some Major Mistakes*, WIRED (May 15, 2017), https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/ [https://perma.cc/8FHR-NXVA].

157. *Innovation and security research*, EUROPEAN COMMISSION (last visited Apr. 11, 2023) https://home-affairs.ec.europa.eu/policies/internal-security/innovation-and-security-research_en.; *see also* Fabiola Schwarz et al., *Empowering Security Researchers Will Improve Global Cybersecurity*, JUST SECURITY (May 6, 2022), https://www.justsecurity.org/81293/empowering-security-researchers-will-improve-global-cybersecurity/ (stating that, "The importance of protecting security researchers was also emphasized at the U.N.-level . . . . The U.N. Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) underlined governments' duty to encourage responsible reporting of vulnerabilities").

158. Katitza Rodriguez et al., *Protecting Security Researchers' Rights in the Americas*, ELECTRONIC FRONTIER FOUNDATION (Oct. 16, 2018), https://www.eff.org/wp/protecting-security-researchers-rights-americas.

159. *Unintended Consequences: Ten Years under the DMCA*, *supra* note 137.

160. *See* Matt Blaze & Steven Bellovin, *Petition to Renew a Current Exemption Under 17 U.S.C. § 1201*, UNITED STATES COPYRIGHT OFFICE (July 22, 2020)

concept, and certain interest, such as security and privacy, should prevail when balanced against the need to protect the rights of copyright owners."[161] Prohibiting unauthorized access to copyrighted work, including when infringement is not the goal, "effectively erase[s] over a century of law that limits copyright to protect free expression."[162]

Notwithstanding the most recent changes in norms concerning vulnerability disclosures, security researchers continue to receive backlash for testing company products; good-faith researchers are constantly on high alert for potential criminal charges. The threat of prosecution stems from two critical sections of federal law: the CFAA and the DMCA.[163] These federal laws "were written to address new forms of crime enabled by new uses of technology, but were written for a fundamentally different digital world."[164] The CFAA and DMCA include penalties central to the act of security testing; however, neither law defines benevolent and malicious actions or actors. Instead, the Copyright Office uses "good-faith" as a condition for a researcher's need to perform security research. Still, this does not leave much (if any) wiggle room because the security research process seems overbearing.

It is difficult to change the public outlook on security researchers when so many companies and laws make it seem like a tool only for "black-hat hackers"[165] However, it is essential to remember that there are benevolent actors who are on the side of technology. Notably, the care and persistence of these actors keep the legal systems from falling too far behind. If not for their discoveries, the public would be

https://www.copyright.gov/1201/2021/petitions/renewal/Renewal%20Pet.%20-%20Security%20Research%20-%20Blaze%20&%20Bellovin.pdf [https://perma.cc/C2AS-JHEM]; *see* Alex J Halderman et al., *Security Research Renewal Pet.*, UNITED STATES COPYRIGHT OFFICE (July 16, 2020), https://www.acm.org/binaries/content/assets/public-policy/ustpc-jt-request-renewal-dmca-security-research-exemption.pdf [https://perma.cc/8SXC-2K69]; *see* The Motor & Equipment Manufacturers Association, *Petition to Renew a Current Exemption Under 17 U.S.C. § 1201 8th Triennial Rulemaking*, UNITED STATES COPYRIGHT OFFICE (July 22, 2020), https://www.copyright.gov/1201/2021/petitions/renewal/Renewal%20Pet.%20-%20Vehicle%20Repair%20-%20MEMA.pdf [https://perma.cc/5FYJ-XYRU].

161. Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 472 (2019) (citing to Helen Nissenbaum, *Where Computer Security Meets National Security*, 7 ETHICS INFO. TECH. 61, 62 (2005) ("Security deserves a place alongside privacy, intellectual property, equity, and other values that have been vigorously debated in light of developments in and application of digital electronic information technologies.")).

162. Kit Walsh, *Copyright Regulator Eases Restrictions on Research, Education, and Repair*, ELECTRONIC FRONTIER FOUNDATION (Oct. 28, 2021), https://www.eff.org/deeplinks/2021/10/copyright-regulator-eases-restrictions-research-education-and-repair-0 [https://perma.cc/QD7Y-JHRC].

163. Tom Brewster, *US cybercrime laws being used to target security researchers*, THE GUARDIAN (May 29, 2014), https://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers [https://perma.cc/5PYP-24B5]; *see* Rachel Treisman, *A Missouri newspaper told the state about a security risk. Now it faces prosecution*, NATIONAL PUBLIC RADIO (Oct. 14, 2021), https://www.npr.org/2021/10/14/1046124278/missouri-newspaper-security-flaws-hacking-investigation-gov-mike-parson [https://perma.cc/NW8C-TBSD]; *see Sunoo Park & Kendra Albert, A Researcher's Guide to Some Legal Risks of Security Research* (2020), https://clinic.cyber.harvard.edu/files/2020/10/Security_Researchers_Guide-2.pdf [https://perma.cc/QUG8-BTCM].

164. Nat Meysenburg, *Cybersecurity Research Should Not Be A Crime: Why We Need Clear, Permanent CFAA and DMCA Exemptions*, NEW AMERICA. (Nov. 18, 2021), https://www.newamerica.org/oti/briefs/cybersecurity-research-should-not-be-a-crime/ [https://perma.cc/R29N-RLE2].

165. Kilovaty, *supra* note 161, at 482 (defining black-hat hacking as hackers who are "motivated by mischief or profit rather than by actually fixing vulnerabilities and security flaws").

obstructed from their free use of technology. For example, in 1947, Grace Hopper[166] found the first computer "bug" and was referred to as a computer pioneer and programmer.[167] Although the bug was just an insect found in one of the parts of the Mark II, computers and bugs have come a long way since 1947.

Interestingly enough, "[t]he chipset that powers your smartphone is smaller and lighter than the moth stuck in the Mark II, and performs computations two or three *hundred million* times faster."[168] Despite the tremendous technological advances we have made in the past seventy-three years since then, more software and hardware bugs have become prevalent in the lines of code on phones and computer devices. In summation: like the evolution of nocturnal moths becoming daytime butterflies[169], computers and computer programs have evolved into more complex systems "creating order out of apparent chaos" and learning to perform logic operations such as the EQU function.[170]

A. *Van Buren v. United States*

As stated, two federal statutes that make finding and fixing flaws in computers and computer programs an even more difficult task are the CFAA and the DMCA. On June 3, 2021, the Supreme Court, in a 6-3 vote, held an individual has "'exceed[ed] authorized access' under the Computer Fraud and Abuse act of 1986, 18 U.S.C § 1030(a)(2), when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders or databases—that are off-limits to him."[171] In *Van Buren*, a Georgia police officer was convicted under section 18 U.S.C. § 1030 (a)(2)(C)[172] of having

166. Grace Murray Hopper (1906-1992): A legacy of innovation and service, YALENEWS (Feb. 10, 2017), https://news.yale.edu/2017/02/10/grace-murray-hopper-1906-1992-legacy-innovation-and-service [https://perma.cc/TY6K-K2VS] (providing a history on Grace Brewster Murray Hopper, who was a computer pioneer and naval officer).

167. *Log Book With Computer Bug*, NATIONAL MUSEUM OF AMERICAN HISTORY (June 30, 2021), https://americanhistory.si.edu/collections/search/object/nmah_334663 [https://perma.cc/LX9F-ZVBQ] (describing Grace Hopper's work on the Mark II computer—an electromagnetic calculating weighting twenty-three tons—at Harvard University, in 1947).

168. Stan Adams, *The Supreme Court and the Copyright Office Have an Important Opportunity to Shore Up Much-Needed Security Research*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Nov. 17, 2022), https://cdt.org/insights/the-supreme-court-and-the-copyright-office-have-an-important-opportunity-to-shore-up-much-needed-security-research/.

169. Moths became daytime butterflies to enjoy the nectar of flowing plants. Nicholas Wade, *How the Butterfly Discovered Daylight*, THE NEW YORK TIMES (Oct. 21, 2019), https://www.nytimes.com/2019/10/21/science/butterflies-moths-fossils-evolution.html. [https://perma.cc/E7JG-FLFK]

170. Sean Pitman, *Computers and The Theory of Evolution*, DETECTING DESIGN (2003), https://www.detectingdesign.com/computerevolution.html [https://perma.cc/Z482-VYWH] (providing insight into the evolution of computer functions); *see* Vladimir Romanov, *PLC Programming Comparison Instructions*, EQUAL https://www.solisplc.com/tutorials/plc-programming-comparison-instructions-equ-equal [https://perma.cc/G3MC-77GQ] (defining and illustrating the Equal or EQU instruction as assigning absolute or relocatable values to symbols—i.e., stating something is "*TRUE* if the two values within 'Source A' and 'Source B' fields are equal to" one another); *see also* Equ instruction, IBM, https://www.ibm.com/docs/en/zos/2.1.0?topic=statements-equ-instruction [https://perma.cc/5V2A-94UB].

171. Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (the first-ever CFAA case to reach the Supreme Court).

172. 18 U.S.C. § 1030 (a)(2)(C) (stating that "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." Generally, however, 18 U.S.C. § 1030 provides that "whoever . . . intentionally accesses a computer

"exceeded authorized access" to the Georgia Crime Information Center database—the requirements for access turns on the computer owner's unilateral policies regarding the use of its network(s).[173] The officer used his valid credentials to search the law enforcement database to retrieve information about a license plate number in exchange for money.[174] The investigation was part of the Federal Bureau of Investigation sting operation.

The charge against Van Buren was "a felony violation of the CFAA on the ground that running the license plate [number] violated the 'exceeds authorized access' clause of 18 U.S.C. §1030(a)(2)."[175] The U.S. Court of Appeals for the Eleventh Circuit affirmed the trial court's decision to sentence Van Buren to eighteen months in prison.[176] On appeal to the Supreme Court, Van Buren argued the CFAA's term "exceeds authorized access" only applies "to those who obtain information to which their computer access does not extend," but not to Van Buren, who "misuse[d his] access that [he] otherwise" had.[177] In his opinion, Justice Barrett wrote that Van Buren did access "the law enforcement database system with authorization."[178] Because Van Buren could use the system to retrieve license-plate information, "[he] accordingly did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose."[179]

The *Van Buren* ruling means the CFAA's "exceeds authorized access" provision only applies to litigants or law enforcement personnel who obtain or use the information to which they do not already have access.[180] The Supreme Court's decision here narrowed the scope of the statute such that the CFAA no longer will provide a cause of action to an aggravated party when an individual member (or group) retrieves or uses electronic information which they have, either previously or contemporaneously been given "access," even if it is for improper use.[181] Although the Court in *Van Buren* discussed the actions under the CFAA, this case also implicates the DMCA.

The parallel between the CFAA and the DMCA appears in their restrictive access provisions. In the CFAA, the standard is "exceeding authorized access," while the DMCA prohibits circumvention of any TPM restricting access to copyrighted work.[182] Conversely, however, the DMCA does not require any

---

without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished . . . [with] a fine [] or imprisonment for not more than ten years, or both").

173. United States v. Van Buren, 940 F.3d 1192, 1207-08 (11th Cir. 2019).

174. Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

175. *Id*. at 1653 (noting that "Van Buren also was charged with and convicted of honest-services wire fraud." This fraud conviction was contrary to the decision in McDonnell v. United States, 579 U. S. 550, 136 S. Ct. 2355, 195 L. Ed. 2d 639 (2016)).

176. *Id*.

177. *Id*.

178. *Id*. at 1662.

179. *Id*.

180. John Moye, *Supreme Court Narrows Scope of Computer Fraud and Abuse Act in Van Buren v. United States*, BARNES & THORNBURG (July 16, 2021), https://btlaw.com/insights/alerts/2021/supreme-court-narrows-scope-of-computer-fraud-and-abuse-act-in-van-buren-v-united-states [https://perma.cc/4T3E-MBSP] (stating that, in other words, not having been granted access means "by accessing directories or databases that they are not authorized to access.").

181. *Id*.

182. Adams, *supra* note 98.

infringement of copyright to hold someone liable.[183] Moreover, even though access controls are relatively universal—for a respective use—it does not fully indicate whether a person is authorized to access particular material.[184] Security researchers are, like everyone else, required to follow the rule of law.[185] However, security researchers should not face criminal liability under the DMCA for conduct that the Copyright Office recognizes as legitimate and having non-infringing value.[186]

B. *Green v. United States DOJ*

Congress developed a new class of rights—a right to control access to copyrighted works, even legitimately acquired copies of such work. It also prohibited trafficking in technology that can circumvent technological measures that protect these works. Independently, these rights alone would have made fair use of digital materials nearly impossible, so Congress added exceptions for specific favored services and users, like law enforcement.[187] Additionally, these new rights provided for a process that allows the public to petition for exemptions to liability under Section 1201 for circumvention.[188]

Green v. United States DOJ is a lawsuit arguing that the DMCA's anti-circumvention provisions prevent legitimate speech under the First Amendment.[189] The D.C. Circuit rejected a First Amendment challenge to the DMCA's anti-circumvention and anti-trafficking provisions. Located in Section 1201(a) of the DMCA, the anti-circumvention provision restricts a person's ability to access, use, or discuss copyrighted materials they purchase.[190] Appellants Dr. Matthew Green, Dr. Andrew Huang, and Alphamax, LLC sought to engage in activities they feared would be prosecuted under the "anti-circumvention" and "anti-trafficking" provisions of the DMCA.[191] In addition to these contentions, the Electronic Frontier Foundation ("EFF") challenged the Library of Congress' triennial rulemaking procedure.[192] EFF argues that the Library of Congress's inability to allow exemptions for using video clips for non-infringing purposes violates the First Amendment and the Administrative Procedure Act.[193]

183. *Id.*

184. *Id*. (e.g., "companies use access controls to prevent interoperability of devices like garage door openers and to prevent farmers from diagnosing and repairing their own tractors, but few would argue that garage door and tractor owners are not authorized to access parts of their own purchases.").

185. Adams, *supra* note 98.

186. *Id*.

187. Catherine Crump & Tait Anderson, *Amicus Brief in Green v. Department of Justice*, BERKELEY LAW (Jan. 19, 2022), https://www.law.berkeley.edu/case-project/green-doj-amicus-brief/ [https://perma.cc/53LH-M7LZ].

188. Crump & Anderson, *supra* note 187.

189. Green v. U.S. Dep't of Justice, 392 F. Supp. 3d 68 (D.D.C. 2019); *see* Kit Walsh, *Green v. U.S. Department of Justice*, ELECTRONIC FRONTIER FOUNDATION (2018), https://www.eff.org/cases/green-v-us-department-justice [https://perma.cc/FF8W-7VNX].

190. Walsh, *supra* note 189.

191. Green v. U.S. Dep't of Justice, 392 F. Supp. 3d at 78 ("exposing them to potential civil liability under the DMCA's private right of action, 17 U.S.C. § 1203, and potential criminal liability under the DMCA's criminal offense provision, 17 U.S.C. § 1204.").

192. Green (EFF) v. DOJ, COPYRIGHT ALLIANCE (2021), https://copyrightalliance.org/copyright-cases/green-v-u-s-dept-justice/ [https://perma.cc/SA7S-9PVT].

193. *Id*.

Dr. Matthew Green is a well-regarded computer science professor, cryptographer, and security researcher at John Hopkins University.[194] Unfortunately, because of Dr. Green's fear of litigation—specifically a claim brought under Section 1201 of the DMCA—he has been unable to conduct "crucial device security research."[195] Dr. Green's developments in "communication systems, financial transaction devices, and medical hardware is virtually important to the integrity and safety of our common infrastructure."[196] Additionally, Dr. Andrew "bunnie" Huang is a world-renown inventor and electrical engineer who has been unable to build on an earlier invention of his due to the threat of prosecution via Section 1201.[197] EFF, on behalf of Dr. Matthew Green and Dr. Andrew "bunnie" Huang (collectively referred to as the "Appellants"), argues two relevant points: 1) the Copyright Office should, as it has in the past, recognize that security-focused exemptions encompass fair use; and 2) the Copyright Office has continued imposing significant limitations on security researchers, thereby hindering their publicly beneficial work.[198]

1. D.C. Circuit Court Rejects First Amendment Challenges

The Office must consider comments, policy proposals, and copyright law and legislation exemptions.[199] Security researchers across the nation have repeatedly gone before the Copyright Office to "secure, renew, and expand" exemptions allowing circumvention of TPMs on copyrighted works resulting from good-faith security research.[200] Since 2006, Dr. Matthew Green and several amici have attended five (5) triennial rulemakings.[201] The Appellants state that the Copyright Office has routinely acknowledged that accessibility-focused exemptions directed at security research encompass fair use but still impose significant limitations on the cybersecurity of products and services.[202] Furthermore, the Appellants argue that the D.C. Circuit should subject Section 1201 to strict scrutiny under the First Amendment. Section 1201 restricts access to information and modifies the equilibrium between free speech and copyright law. Content-based exceptions, in

194. Matthew D. Green associate professor department of computer science Johns Hopkins University, Matthew D. Green, https://isi.jhu.edu/~mgreen/ (providing that Dr. Green is a founder of Sealance, which enables regulatory compliance for digital assets, and he "developed protocols that allow users access databases without revealing *which* data they're accessing.").

195. *After Three-Year Wait, Court Allows First Amendment Challenge to Copyright Law to Proceed*, JDSUPRA https://www.jdsupra.com/legalnews/after-three-year-wait-court-allows-37403/.

196. Walsh, *supra* note 189.

197. Dr. Huang and AlphaMax, LLC (his company) were attempting to advance the quality of the NeTV2—a digital video processing device allowing the users to record and modify video data derived from sources including streaming services and video games. The current version of NeTV2 is unable to change encrypted video streams, so Dr. Huang and AlphaMAx, LLC attempted to include this feature by reverse engineering Intel's High-Bandwidth Content Protection copy protection system. The DMCA Section 1201 concerns, however, have stunted this project.

198. Brief for Matthew D. Green, et al. as Amicus Curiae, at 10, Green v. U.S. Department of Justice, (2022) (No. 21-05195) [hereinafter Brief for Matthew D. Green, et al.].

199. Overview of the Copyright Office, *supra* note 86.

200. Brief for Matthew D. Green, et al. at 15.

201. Brief for Matthew D. Green, et al. at 15 (citation omitted).

202. Brief for Matthew D. Green, et al. at 15–16. The critics, such as the EFF, argue this new right dramatically increased the power that manufacturers have regarding their products, to the determinant of consumers.

1201 and through the triennial review process created by Section 1201, mean the court should subject the statute to strict scrutiny.

Conversely, the DOJ and other copyright advocates like Intel Corp. and Motion Picture Association Inc. argue that Section 1201 advances the digital economy.[203] "Content creators can better market their work with paywalls and other systems that protect their work from infringement." [204] Devlin Hartline, a legal fellow at the Hudson Institute specializing in intellectual property[205], stated: "[c]ongress realized that copyright owners need a safe place where they'll want to share their works in digital form." Additionally, Mr. Hartline suggests that Section 1201 was created to "protect these digital locks in order to prevent infringement from happening in the first place."[206]

Appellants in *Green* brought a pre-enforcement action challenging the DMCA on facial and as-applied First Amendment grounds.[207] The district court held that Dr. Green's planned publication was unlikely to implicate Section 1201(a) as a result of the book being designed, used, and marketed for educational purposes (as opposed to purposes of circumvention).[208] On the other hand, the district court denied Dr. Huang's request for preliminary injunctive relief, finding that he was unlikely to succeed on his as-applied claim.[209]

The court, when addressing the merits of the case, provided that "'[i]n First Amendment cases, the likelihood of success will often be by the determinative factor in the preliminary injunction analysis.'"[210] For Dr. Huang to succeed on the merits, he must be able to show that the DMCA is unconstitutional as it is applied to his alleged speech activity. This is a three-step process where the court first begins with deciding if "'[the activity at issue] is speech protected by the First Amendment.'"[211] Then, the court examines whether the regulation is content-based or content-neutral.[212] "This sets the level of scrutiny we apply at the third step: strict scrutiny for content-based statutes and intermediate scrutiny for content-neutral statutes."[213]

The analysis under step one was relatively straightforward. The NeTVCR device Dr. Huang wishes to sell contains a "code signed to circumvent certain access controls."[214] The device's purpose is to allow those possessing an earlier model of

203. Isaiah Poritz, *Anti-Hacking Copyright Law Scrutinized in Free Speech Challenge*, BLOOMBERG LAW (Sept. 12, 2022), https://news.bloomberglaw.com/ip-law/anti-hacking-copyright-law-scrutinized-in-free-speech-challenge [https://perma.cc/VFP9-UFT3].

204. *Id*.

205. *See* Devlin Hartline, HUDSON (maintained 2022), https://www.hudson.org/experts/1394-devlin-hartline [https://perma.cc/EY3T-ABFG] (Mr. Hartline holds a JD and an LLM, with concentrations in intellectual property and constitutional law. Mr. Hartline also holds a BA in mathematics).

206. Poritz, *supra* note 203.

207. Green v. United States DOJ, U.S. App. LEXIS 33559, at 6.

208. *Id*. at 7.

209. *Id*. at 7-8 (stating "that the district court favorably cited the Second Circuit's analysis in *Universal City Studios, Inc. v. Corley*—the only decision by a circuit court to have squarely addressed the constitutionality of the DMCA").

210. *Id*. at 11 (citing Pursuing America's Greatness v. FEC, 831 F.3d 500, 511 (D.C. Cir. 2016)).

211. *Id.* (citing Cornelius v. NAACP Legal Defense & Education Fund, Inc., 473 U.S. 788, 797 (1985)).

212. *Id.* at 11–12 (citing City of Austin v. Reagan National Advertising of Austin, LLC, 142 S. Ct. 1464, 1471 (2022) (asking whether it applies specifically to a particular speech due to the topic discussed or the idea that is expressed)).

213. *Id*. at 12 (citing Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 641-42 (1994)).

214. *Id.* (citing Appellants' Reply Br. 10; Oral Arg. Rec. 13.15-13.40).

his instrument to edit and improve his code.[215] Dr. Huang argues that "writing and communicating computer code capable of circumventing [TPMs] qualifies as First Amendment-protected speech."[216] The government, however, had conceded during oral arguments that "if you write code so somebody can read it," it is "expressive" speech.[217] Other courts found the First Amendment protects "[i]nstructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both)."[218] As such, "because computer source code is an expressive means for the exchange of information and ideas about computer programming," it is thereby protected by the first amendment.[219]

The analysis under step two asked whether the DMCA "'target[s] speech based on its communicative content'—that is, if it 'applies to particular speech because of the topic discussed or the idea or message expressed.'"[220] In holding that the DMCA does not target speech based on its communicative content, the court reasoned that the anti-circumvention and anti-trafficking provisions only target the act of circumvention and provisions of circumvention-enabling tools.[221] To provide certainty, the DMCA may indirectly increase the difficulty of expressing things with computer code, so long as that code facilitates circumvention and expressive activity is not the statute's target.[222] [T]he DMCA "is [not] concerned with whatever capacity [code] might have for conveying information to a human being." Instead, it applies to code "solely because of its capacity to instruct a computer."[223]

Although the DMCA requires reading computer code to establish what digital act the code carries out, it is content neutral because it cares about the expressive message in the code "only to the extent that it informs" the code's function.[224] The code's "substantive message itself is irrelevant."[225] As such, the court concluded that the DMCA survives the content-neutral and intermediate scrutiny test.[226]

---

215. *Id.*

216. *Id*.

217. *Id*. at 20.

218. *Id.* at 12–13 (quoting *Corley*, 273 F.3d at 448).

219. *Id.* at 13 (quoting Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000)).

220. *See* City of Austin v. Reagan National Advertising of Austin, LLC, 142 S. Ct. 1464, 1471 (2022) (quoting Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015)).

221. *See* 17 U.S.C. § 1201(a)(1)(A) ("No person shall circumvent a technological measure that effectively controls access to a [copyrighted work.]"); *Id.* § 1201(a)(2) ("No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any [circumvention technology or product].").

222. Green v. United States DOJ, U.S. App. LEXIS 33559, at 13.

223. *Id*. at 13-14 (quoting *Corley*, 273 F.3d at 454).

224. *Id*. (quoting City of Austin v. Reagan National Advertising of Austin, LLC, 142 S. Ct. 1473 (2022)).

225. *City of Austin*, 142 S. Ct. at 1472.

226. Green v. United States DOJ, U.S. App. LEXIS 33559, at 15-17.

Huang's NeTVCR device would, by design, "permit virtually anything displayable on a modern television screen to be recorded in the clear and made available online" by making obsolete the technological protection measure it targets. Copyright Office, *Section 1201 Rulemaking: Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention* 143 (2018). This would "eviscerate virtually every single video content delivery protection system exposing valuable copyrighted video content to massive infringement," [], gutting the government's substantial interest in ensuring the broadest distribution of copyrighted materials. Huang, who spends most of his brief addressing strict scrutiny, offers no meaningful response and is thus unlikely to succeed on the merits.

Dr. Green voiced his concerns with the threat of prosecution for publishing his academic book "to instruct readers in the methods of security research," which will include "examples of code capable of bypassing security measures."[227] The court held that the government's concession ends any "credible threat of prosecution" against Dr. Green.[228] Therefore, he is left without standing to obtain a preliminary injunction. Moreover, the court held that Dr. Huang's arguments on the outstanding preliminary injunction factors rest entirely on his flawed claim that continued enforcement of the DMCA imperils his First Amendment rights.[229]

2. Non-Applicability of the Administrative Procedures Act

The court held that the triennial rulemaking process does not adhere to the Administrative Procedure Act ("APA").[230] The Appellants argued that the Library of Congress, the Librarian of Congress, the Copyright Office, and the Register of Copyrights violated the APA by refusing "portions of the exemptions that apply to [Dr.] Green's security research" as well as "the exemptions that would have applied to [Mr.] Huang and Alphamax's creation and use of NeTVCR" through the 2015 triennial exemption rulemaking proceedings.[231] While the Copyright Act subjects the Register of Copyrights to the APA, the court held that "the APA only applies to a 'final agency action,' and the triennial rulemaking process is consummated by the Librarian of Congress (based on the recommendation of the Register). The Librarian is not subject to the APA."[232]

For an agency action to be held as "final," "the action must mark the consummation of the agency's decision process," as well "the action must be one by which rights or obligations have been determined, or from which legal consequences will follow." [233] The Librarian of Congress, acting on behalf of the Library of Congress, "consummates" the triennial exemptions to the DMCA's circumvention prohibition and is required only to consider "recommendation[s] of the Register of Copyrights" during the exemption process[234], the disputed "final" action at issue here is one taken by the Librarian and Library of Congress.[235] Consequently, the statutory provision holding the activities of the Register of Copyrights to the APA[236] prohibits related claims against the Copyright Office and Register of Copyrights for any agency action taken per the DMCA's triennial rulemaking process.[237]

227. *Id.* at 9.

228. *Id*.

229. *Id*. at 17 (affirming the district court's denial of Green and Huang's motion for a preliminary injunction and remand for further proceedings consistent with this opinion).

230. Green (EFF) v. DOJ, *supra* note 192.

231. *Green v. U.S. Dep't of Justice*, 392 F. Supp. 3d at 96.

232. Green (EFF) v. DOJ, *supra* note 192.

233. *Bennett v. Spear*, 520 U.S. 154, 177-78, 117 S.Ct. 1154, 137 L.Ed.2d 281 (1997) (internal quotation marks omitted).

234. 17 U.S.C. § 1201(a)(1)(C).

235. *Green v. U.S. Dep't of Justice*, 392 F. Supp. 3d at 96–97.

236. *See* 17 U.S.C. § 701(e).

237. *See Green v. U.S. Dep't of Justice*, 392 F. Supp. 3d at 97.

VI. SUGGESTIONS GOING FORWARD

Understanding what cybersecurity is, the purpose of security research, and the courts' interpretations on these matters, are essential to developing reasonable regulations addressing the issues surrounding security research and vulnerability reporting. By now, we see that the DMCA's evolution through its years of rulemaking provides that the process is often limiting and cumbersome. Lawmakers and regulatory groups should recognize the benefits of security research and acknowledge that keeping a tight leash on ethical hacking gives malicious actors the upper hand in identifying and exposing security threats.

Depending on how old you are, many of us saw and participated in the recent rise of everyday mainstream technology usage. The 2010s, for example, gave rise to social media, cloud computing, and artificial intelligence—fundamentally changing our day-to-day lives. The list of innovations from that decade could span miles. However, and more importantly, their contribution to the public was (and continues to be) worth more than we can put into words. iPads, smartwatches, fitness trackers, wireless earphones, virtual assistants, and so on have started bringing sci-fi tropes to life. All of this was thought to be impossible just a few decades ago. In the fast-paced world of tech, however, these advancements occur so often now that our lives today are not the same as they were even a year ago.

If the technological landscape changes so quickly each year, the laws that govern society should not be expected to reflect even a small percentage of these changes. The DMCA was written in 1998 and has since undergone multiple rounds of evolution—via three-year cycles of rulemaking proceedings. Therefore, updating laws to reflect modern technological threats should be the first area of attention. Section 1201 should be rewritten to deviate from its existing process for requesting and granting temporary exemptions every three years. Particularly, the anti-circumvention and anti-trafficking provisions need reforms to create permanent protections for researchers not looking to violate copyrighted work products.

In addition to the ones below, several potential solutions address the issues posed by Section 1201 of the DMCA to security researchers. Special consideration should be given to the creation of exemptions. The Library of Congress has the authority to grant exemptions to the ban on circumventing TPMs, but this process can be slow and limited. Making the exemption process easier and granting broader exemptions for security research activities could help address some concerns around Section 1201. Moreover, consideration could be given to possible legislative reform. Changes to the language of the law could provide more clarity and protection for security researchers investigating systems to improve security. This could include a clear definition of what constitutes "authorized" security research and a provision that shields security researchers from liability for circumvention of TPMs for security research.[238] Lastly, consider whether there should be any industry

238. *C.f.* Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (proposed March 23, 2022) (Proposing rules regarding disclosures of cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Commission ("SEC"). Under the proposed rules, Proposed Item 1.05 requires material cybersecurity incidents to be disclosed within four business days after the registrant determines a material "cybersecurity incident" has occurred. Registrants are not expected to provide detailed technical information that "would impede [the] response or remediation of the incident." Importantly, through practical consideration, information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information

best practices. Companies can adopt best practices that encourage and support security research, such as implementing bug bounty programs and creating a transparent process for reporting and addressing vulnerabilities. Ultimately, combining these solutions could help create a more supportive and secure environment for security researchers to conduct their work while also protecting the rights of copyright holders.

A. Short-Term Solution

Section 1201 of the DMCA has caused significant concern among security researchers and the cybersecurity community. This provision of the law makes it illegal to circumvent technological measures that control access to copyrighted works. While this provision was intended to prevent piracy, it has been criticized for hindering the work of security researchers and potentially putting computer systems and users at risk. In this section, we will explore some short-term solutions that security researchers can use to protect themselves from the restrictions imposed by Section 1201 of the DMCA.

Starting with the dogged three-year delay between hearings: for new recommendations and exemptions, the Office should attempt to streamline existing exemptions. Every three years, the Library of Congress holds a triennial rule-making process during which security researchers and other stakeholders can apply for exemptions to specific provisions of the DMCA. This allows security researchers to engage in activities otherwise restricted by the law. For example, in the past, exemptions have been granted for activities such as testing automotive systems and jailbreaking smartphones. Security researchers can participate in this process by submitting comments or participating in public hearings. Nevertheless, obtaining, or renewing exemptions from the DMCA is a tedious and complex process. While the Office is well within its reason to address exemptions on copyrighted work (with some glaring discretion), security researchers with legitimate purposes suffer due to this overly complicated process.

Streamlining existing exemption procedures will provide for a proactive approach by security researchers when examining copyrighted software. The promising result would be to identify more vulnerabilities by loosening the leash on non-permissible actions of Section 1201. Based on this streamlined model, a proponent of an exemption must file a renewal request(s) with circumstantial evidence that the exemption should still be valid. Proof of prior exemptions, for example, could be fastened to the application. Consideration of a neutral scheme would involve allowing adversaries of the exemption to provide evidence to the Office of why the renewal request is invalid. After considering evidence from both parties and absent objections, the Office may announce final decisions as to the renewal being valid for its stated purpose(s).

Another solution that security researchers can use is to rely on the protection provided by legal safe harbors (discussed in more detail below). For example, the CFAA protects security researchers who engage in penetration testing as long as

made available." Jeff Johnston et al., *What Makes a Cybersecurity Risk or Incident Material? A Look at the SEC's Proposed Rules on Cybersecurity*, INSIGHTS (Jan. 27, 2023), https://www.velaw.com/insights/what-makes-a-cybersecurity-risk-or-incident-material-a-look-at-the-secs-proposed-rules-on-cybersecurity/ [https://perma.cc/TUC7-J4P2] (Quantitative and qualitative factors determine whether an incident is material in light of the specific circumstances presented).

they have obtained permission from the owner of the targeted system. Similarly, the anti-circumvention provisions of the DMCA provide some protection for security researchers who engage in activities such as vulnerability research if they do not engage in activities such as piracy or illegal file sharing.

In addition, security researchers can take steps to maintain their privacy and anonymity. Maintaining privacy and anonymity can include using encrypted communication channels, using pseudonyms, and avoiding releasing sensitive information that could be used to identify them. Ultimately, it can protect security researchers from legal or other forms of retaliation and help them focus on their research without distractions. Moreover, security researchers should obtain written permission from the owner or authorized agent of a copyrighted work before conducting research that may involve accessing or circumventing the work. This can help protect security researchers from legal action, as it provides evidence that they acted with the permission of the owner of the copyrighted work.

Finally, security researchers can seek legal counsel from an attorney experienced in digital copyright and security research. This can help them better understand their research activities' legal implications and take appropriate steps to minimize legal risk. An attorney can also guide on other issues, such as protecting sensitive information, using pseudonyms, and preparing written agreements with stakeholders.

In conclusion, security researchers face significant challenges in navigating the restrictions imposed by Section 1201 of the DMCA. However, several short-term solutions can help protect security researchers and allow them to continue their essential work. These solutions include the exemption process, reliance on legal safe harbors, maintaining privacy and anonymity, obtaining written permission, and seeking legal counsel. By utilizing these tools, security researchers can continue their work without fear of legal repercussions and can help protect computer systems and users from potential security threats.

B. Incentivizing Ethical Hackers

Under the existing resources, security researchers should be incentivized to conduct ethical hacks and report vulnerabilities that the vendor would otherwise be unaware of.[239] Reporting to vendors would lower the number of unpatched vulnerabilities and reduce the opportunities for adversaries to attack company programs. Stemming from this, more industries would likely invest additional resources in cybersecurity programs to develop secure devices "as companies will attempt to avoid public shaming based on flaws in their software detected by ethical

239. Safe harbor provisions incentivize security researchers to engage in ethical hacking, assuring them that their work will not result in legal consequences, even if they inadvertently discover copyrighted material. This is an important consideration, as the protection offered by the DMCA provides an essential safeguard for the public. In addition, ethical hacking helps to identify security vulnerabilities and protect against cyber-attacks, which can cause widespread harm to individuals, businesses, and governments. By incentivizing ethical hacking, the DMCA helps to ensure that security researchers can perform their work effectively without fear of legal repercussions. So, the provisions of the DMCA that protect security researchers who engage in ethical hacking play an essential role in promoting online security and protecting against cyber-attacks. By providing legal protection for ethical hackers, the act incentivizes security researchers to engage in this critical work, helping to ensure that our online systems and networks are secure and protected against malicious actors.

hackers."[240] It is essential to understand that this would, by no stretch of the imagination, completely prevent malicious hacking. Alternatively, it is a suggestion to reduce the likelihood of malicious acts—increasing the cost associated with mounting a cyber-attack and enabling additional targeting and efficient law enforcement efforts to address them with greater liability.[241] To attain this goal, we must create bold divisions between malicious and benevolent actors. As well as administrative and legislative reformations "such as clarifying the boundaries of the CFAA and DMCA in relation to security research."[242]

Moreover, companies should be grouped by industry to come up with a consensus on how they would like to disclose vulnerabilities, followed by seeking the help of security research professionals to determine the most feasible manner(s) suggested. Currently, the model behind disclosures is patchy and fact-dependent, with the disclosure causing legal threats against security researchers. However, structured disclosure with adequate communication between knowledgeable parties and attention to remedying a flaw reduces the risk of legal repercussions. In *Taking The Pulse of Hacking: A Risk Basis for Security Research*, Joseph Lorenzo Hall and Stan Adams recommend that to reduce personal risks associated with vulnerability disclosure, security researchers should consider remaining anonymous and instead refer to intermediaries to handle disclosures.[243] Although this suggestion is helpful, revisiting the fundamental discrepancies between disclosure practices is still paramount to resolving the issues.

Lastly, security researchers should be supported in their attempt to create modifications to help patch flaws in software systems. "Such modifications might include requiring that vendors embed built-in patchability into [Internet of Things ("IoT")] devices, using privacy tort law to address potential externalities associated with security research, tackling vendors who employ the 'security by obscurity' practice."[244] Professional relationships between companies and researchers and contractual obligations (such as non-disclosures and non-compete agreements) are already uneasy.[245] Ensuring researchers have the support of government agencies will reduce the chilling effects on a researcher's choice of project.

C. Proposed Safe Harbor

Although the Copyright Office meets every three years to discuss the importance of adopting exemptions to the DMCA's ban on circumvention, the laws

240. *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L. REV. 2442, 2450 (2006) ("[M]edia coverage, and user complaints can prompt vendors to take action" otherwise, "vendors would be more complacent.").

241. *See generally* Kilovaty, *supra* note 161 at 472. ("IoT devices enable not only data about direct computer use but also data about driving, home heating and cooling, food stored in a refrigerator, pulse and blood pressure, sleep patterns, and much more.").

242. *Id*. at 505.

243. *See generally* Joseph L. Hall & Stan Adams, *Taking The Pulse of Hacking: A Risk Basis for Security Research*, CENTER FOR DEMOCRACY & TECHNOLOGY (March 2018), https://josephhall.org/papers/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf [https://perma.cc/5BJ4-KDAJ] (suggesting that in cases where "downloading data is an important part of vulnerability handling, to minimize risk, researchers should practice data minimization techniques, making an effort to download only enough for the relevant analysis, and securely disposing of it afterwards.").

244. *See* Kilovaty, *supra* note 161.

245. Hall & Adams, *supra* note 243.

surrounding vulnerability reporting remain uncertain. Many vendors have bug bounty programs[246] that provide hackers a way of reporting security vulnerabilities directly to allow affected companies a way to patch the problem before malicious actors learn of it.[247] Even so, companies are not overly fond of being notified of these types of reports.[248] Statutory safe harbors should be considered for protecting security researchers who are at the mercy of unhappy companies.

The template of the safe harbor should rest on a responsible disclosure model that has the researcher and vendor engage in constructive communication.[249] This model would emphasize cooperation. In providing a solid platform for communication and vulnerability classification, the security researcher would maintain a greater level of control regarding the publication timeline, allowing for publication regardless of the vendor having patched a breach.[250] All security researchers are granted safety from legal consequences so long as they remain within the safe harbor restrictions.

The safe harbor would include "the researcher disclosing the discovered vulnerability to the vendor first, waiting a mutually negotiated amount of time" for the vendor to patch, "then exercising her right to publicly disclose the vulnerability."[251] However, research regarding security standards— rather than subjecting specific products to an analysis—would not violate Section 1201.[252] Because the standards are promulgated openly, outsiders can engage in security research. Often, vendors confuse this form of research with those that explore particular vendor products. This is where many researchers fall into trouble because vendors threaten legal action.[253]

Determining the safe harbors interplay with the DMCA would act as a default rule—exempting a security researcher from liability under Section 1201. Importantly, the safe harbor shall act as an addition to, rather than a replacement to, the exception in Section 1201 (j).[254] Each vulnerability would be placed in qualified

246. Bug bounty programs are common ways for ethical hackers to earn rewards (i.e., monetary) for successfully discovering vulnerabilities or bugs, and reporting their findings to the appropriate vendor (e.g., app developers). *See Bug Bounty Programs*, HACKERONE (last visited Jan. 7, 2022), https://hackerone.com/bug-bounty-programs [https://perma.cc/3DD6-Q9UF] ("Bug bounty programs allow companies to leverage the hacker community to improve their systems' security posture over time").

247. *See* Charlie Osborne, *Disclose.io: A safe harbor for hackers disclosing security vulnerabilities*, ZDNET (June 1, 2018), https://www.zdnet.com/article/disclose-io-a-safe-harbor-for-hackers-involved-in-vulnerability-disclosure/ [https://perma.cc/C3D4-XUTE].

248. *See* Daniel Etcovich & Thyla van der Merwe, *Coming in from the Cold: A Safe Harbor from the CFAA and the DMCA §1201 for Security Researchers*, ASSEMBLY PUBLICATION SERIES, BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY, HARVARD UNIVERSITY (June 2018), https://dash.harvard.edu/handle/1/37135306 [https://perma.cc/U6NC-RQW2].

249. *See id*.

250. *See id*.

251. *Id*.

252. *Id*.

253. Daniel Etcovich & Thyla van der Merwe, *supra* note 248.

254. 17 U.S.C. § 1201 (j)(3)(a–b). Under subsection (j), to be exempt one must meet the following: determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include . . . (A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and (B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

periods where disclosure is permissible. Questions about how these disclosure periods would be determined would fall under the Department of Justice ("DOJ"). As the federal government's primary law enforcement entity, the DOJ is interested in computer security research.

The DOJ brings enforcement of the DMCA when there are violations of the anti-circumvention provisions in Section 1201.[255] Although some claims brought are justified, the Computer Crime and Intellectual Property Section ("CCIPS")[256] has recognized that not every effort to circumvent TPMs is "illegitimate."[257] Additionally, the DOJ benefits from authorized criminal investigation activities. For example, a benefit would be an order to access password-protected networks that have data relevant to criminal investigations.

Although the DMCA was created to protect copyrighted works, its reasonable relation to those works ends when considering TPMs. The DOJ is better suited to control Section 1201 (i.e., to determine the applicable periods for permissible disclosure) because it is responsible for prosecuting intrusions into computers, damage to information systems, and related offenses.[258] The DMCA is not the primary legal protection to prevent malicious tampering with those devices. It is logical that "malicious tampering with certain devices or works" results in legal prohibitions; however, it is against public policy to enforce the same legal prohibitions for minor acts without malicious intent.[259] The Office also conflates major and minor acts and makes no distinction between benevolent and malicious actors. It must do so because it creates the rules and rightly so wishes to enforce them. But the Office is not an entity meant to have sole power over enforcing these rules. Alternatively, its purpose is to create rules that other entities (and agencies) tasked with considering public policy in practice look to when deciding whether to bring legal action.

D. Unraveling Benign & Malicious Hackers

Notwithstanding its harsh provisions, the DMCA strives to establish a line between malicious and benevolent hackers. But, of course, this is much easier said than done. The issue with the suggestion that security researchers should be protected from legal obstacles is that it is difficult to precisely determine who acts maliciously and benignly in cyberspace.[260]

How to characterize and measure maliciousness is subject to different schools of thought. Historically, cybersecurity research focused on malicious attacks on some software representative of all hackers. There are, however, alternative considerations. "In modeling cyber threat risk, human factors are often overlooked

255. John T. Lynch Jr, *USDOJ Letter to USCO*, US DEPARTMENT OF JUSTICE CRIMINAL DIVISION (June 28, 2018), https://www.copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf [https://perma.cc/RNB4-5AC6].

256. The CCIPS is a subsect of the DOJ's Criminal Division.

257. Lynch, *supra* note 255.

258. *Id*.

259. *Id*.

260. *See generally* Larisa April Long, *Profiling Hackers*, SANSANS INST. INFOSEC READING ROOM 6 (Jan. 26, 2012), https://sansorg.egnyte.com/dl/f0iweQFaQF [https://perma.cc/2VLZ-3GEQ] ("While the law is clear concerning hacking, the definition gets a bit fuzzy among the general population and even computer professionals. Added into this mix are the Gray Hats, or Ethical Hackers, who blur the line between White and Black.").

due to their difficulty of analysis and lack of accessible data."[261] To determine precisely when malicious behavior is to occur, it is suggested that the best course of action is "to characterize each and every individual and make note of patterns in individual attributes increase their risk of behaving maliciously."[262] Unfortunately, this approach is not feasible for most companies.

Alternatively, the distinction should be focused on "weaponization and exploitation—whether the hacker simply identified a flaw and reported it responsibly to the vendor (ethical hacking), or whether she or he exploited it to cause damage (malicious hacking)."[263] We would take this approach to examine whether companies have the resources to review each assessment. If so, the expertise of third parties or inside hires would help determine what tools and techniques were used to expose the vulnerability. At that point, the level of severity would be determined by using a risk classification program to assess the harm given the specific circumstance.[264] This is a retrospective approach that requires a high level of detail; it ultimately would pay off by allowing programs and ethical hackers to identify common trends related to malicious hacking.

The nature of the vulnerability is mainly determinative of whether the hacker is acting ethically or maliciously. By exploiting the vulnerability, the likely assumption is that the hacker is motivated by a desire to monetize the vulnerability such that it causes harm to unsecure computer networks.[265] Although, a significant amount of time and resources are required to exploit vulnerabilities.[266] In the time between initially attempting to exploit and exploiting, the appropriate law enforcement would need to take the proper action to prevent ancillary harm.[267]

E. Rethinking Who Governs the DMCA

The debate as to whether the Library of Congress and the Copyright Office have the requisite expertise to create laws regarding anti-circumvention and technology is never-ending. As a result, many have suggested that the DMCA should shift to another agency or organization consisting of experts in the digital field. Allowing

261. Zoe M. King et al., *Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment*, FRONTIERS IN PSYCHOLOGY (Feb. 5, 2018), https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00039/full [https://perma.cc/5VCA-8XK8].

262. *Id*.

263. *See* Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 239, 244 (2013) ("As an alternative to engaging in 'responsible disclosure,' a researcher could instead 'exploit' or weaponize the 0-day vulnerability.").

264. *E.g.*, Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and: (1) the data is intended for public disclosure, or (2) the loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on the company's mission, safety, finances, or reputation. Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and: (1) the data is not generally available to the public, or (2) the loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the company's mission, safety, finances, or reputation. Data and systems are classified as High Risk if: (1) protection of the data is required by law/regulation, (2) the company is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or (3) the loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on the company's mission, safety, finances, or reputation.

265. *See* Paul N. Stockton & Michele Golabek-Goldman, *supra* note 263.

266. *Id*.

267. *See id*. ("Transforming a vulnerability into a weaponized exploit may require significant investments of time, money, and resources.").

experts in this field to govern over the DMCA, as opposed to the Library of Congress, would be advantageous for software owners and users. Arguments in favor of this shift further state that, acting as a neutral party, Congress does not retain the minimum expertise required to resolve intricacies for software circumvention.[268]

Various security agencies focus on cybersecurity issues and ways to protect the public from cybercrime attacks. So, a strongly recommended solution would be for Congress to delegate any agencies with authority to oversee the DMCA. For example, suppose Congress wants to ensure that no one agency has a monopoly over copyright regulations. In that case, it could create a committee of digital and cyber experts to regulate and govern the DMCA.[269]

Looking closely at the purpose behind the Copyright Office and Library of Congress, their functions are not on copyright per se; instead, they govern works already protected under copyright. In order to invoke protections under the DMCA, a product must be copyrighted; the copyright only acts as a gate to utilizing the DMCA. What does this mean? The DMCA is not, on its own, a copyright law. Where "'copyright is a property based model,'" the "'DMCA controls access to the copyrighted property and prohibits circumvention of the copyrighted words.'"[270]

Moreover, when the DMCA is violated, claims raised do not have to comply with the requirements under copyright law. It boils down to this: making or distributing unauthorized copies of copyrighted material shall break federal law that imposes severe civil or criminal penalties if/when caught. Striping the DMCA from the authority of the Office and the Library of Congress is, therefore, a reasonable suggestion.

Expanding on the idea of separating the DMCA from its current regulators, the DMCA could become its own specific jurisdiction.[271] This would mimic the exemplary standard created for Patents in the Federal Circuit Courts.[272] In addition, by providing the DMCA with its authority, digital experts would be at the head of court hearings—eliminating the uncertainty current Copyright Office and Library of Congress members have about how the DMCA should impact copyrighted work.

An additional argument for removing (or severely amending) the DMCA would be regarding Article I. Magnifying the Copyright Office to allow flexibility in regulatory copyright law requires Congress to establish a new entity. This solution falters because the Copyright Office is a subsidiary of the Library of Congress. As such, it is an Article I agency.[273] By providing the Librarian of Congress, as well as the Register, rulemaking authority under DMCA, Congress violated the

268. The DMCA must have input from experts in the respective field. Although 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).

269. *Cf.* Ross Schulman, *Deeplinks Blog*, ELECTRONIC FRONTIER FOUNDATION (Jan. 30, 2023), http://www.eff.org/deeplinks/2011/11/house-committee-rushing-approve-dangerous-information-sharing-bill [https://perma.cc/S8S3-KJMX] (providing examples of recent U.S. cybersecurity legislative initiatives).

270. Katherine Weigle, *How the Digital Millennium Copyright Act Affects Cybersecurity*, 9 AM. U. INTELL. PROP. BRIEF 3–4 (2018) *(citing* Arielle Singh, *Agency Regulation in Copyright Law: Rulemaking Under the DMCA and Its Broader Implications*, 26 BERKELY TECH. L.J. 527–28 (2011).

271. S*ee id*.

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

273. *See* 17 U.S.C. § 701 (granting powers to the Copyright Office and the Register, under the authority of Librarian of Congress, who appoints the Register and her subordinates).

aggrandizement principle and, significantly, the separation of powers doctrine. Although Congress retains lawmaking power under Article I, notice and comment procedures do not adhere to the requirements under Article I for lawmaking.[274] As a result, the Copyright Office has consistently been influencing legislative rules, and there is no separation of power.[275]

The Copyright Office has broad discretion over the DMCA. As such, Congress may consider scaling back the Office's responsibilities. If dismantling Section 1201 is the extreme solution, several other solutions are worth looking into. Considering previous rulemaking efforts, the statutory exemptions regarding security testing, reverse engineering, and encryption research should be expanded by Congress.[276] As well, Congress should consider new or expanded permanent statutory exemptions. New or expanded permanent exemptions may address the concerns regarding repair and unlocking, which have been prominent since DMCA's birth.[277] A more robust consideration would be for Congress to exempt circumvention that lacks a causal link to infringement[278] or circumvention undertaken by owners of devices.[279] The unjust effects of Section 1201 have harmed people—both directly and indirectly. Congress "should take responsibility for the overbreadth of the anti-circumvention rules" instead of considering changes every three years and creating more ambiguity.[280]

Alternatively, suppose Congress refuses to intervene with the duties and powers granted to the Copyright Office regarding the DMCA. In that case, the Copyright Office should take it upon itself to provide temporary exemptions, as opposed to the narrowly defined exemptions currently provided for.[281] A substitute approach relieves the Copyright Office from needing to resolve cybersecurity and data privacy law questions beyond their expertise and not violating anti-circumvention provisions.[282] The Copyright Office must provide consumers and researchers facing uncertain liability with some reassurance and clarity that security research does not

274. *See* Metro. Wash. Airports Auth. v. Citizens for the Abatement of Aircraft Noise, 501 U.S. 252, 277 (1991) (holding that for a legislative official to pass a law, it must pass both houses and must be subject to the presidential veto).

275. *See* Singh, *supra* note 106, at 531–32.

276. *See* Section 1201 of Title 17, A Report of the Register of Copyrights, UNITED STATES COPYRIGHT OFFICE (June 2017), at 128, https://www.copyright.gov/policy/1201/section-1201-full-report.pdf [https://perma.cc/QS7B-3UMX] (The US Copyright Office recommends that Congress broaden current statutory exemptions and create new ones, a solution that would lessen, though not eliminate, the burden the Office carries in the rulemaking).

277. *Id*. at 88–99.

278. Aaron K. Perzanowski, *The Limits of Copyright Office Expertise*, 33 BERKELY TECH. L.J. 733, 736 (2018), (citing *Chamberlain Group, Inc. v. Skylink Techs.*, Inc., 381 F.3d 1178 (Fed. Cir. 2004) (holding that a claim for circumvention requires a "critical nexus" to copyright infringement)); *see also* Pamela Samuelson, *The Copyright Principles Project: Directions for Reform*, 25 BERKELY TECH. L.J. 1175, 1205 (2010).

279. *Id*. at 766-767. (citing Aaron Perzanowski & Jason Schultz, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY, 147 (Laura DeNardis & Michael Zimmer eds., 2016)).

280. Perzanowski, *supra* note 278.

281. *See id*.

282. *See generally*, Apple Inc. v. Corellium, LLC, No. 19-81160-cv, 2020 U.S. Dist. LEXIS 136419, at *11–12 (S.D. Fla. July 30, 2020) (allowing Dr. Siegel to testify as an expert witness on "good faith security research," due to his qualifications in the cybersecurity industry. In permitting Dr. Siegel to testify, the Court stated that an "average layperson would not understand [security research] standards or the security research industry").

violate Section 1201.[283] Suppose the Office considers the views established and followed by the Department of Transportation or the Food and Drug Administration[284] In that case, there is a near certainty that the Office will exceed its expertise.[285] Those views on the advisability of technological controls are beyond the Office's ability to adapt. Although the Copyright Office has been hesitant to entertain this idea, determining "whether or not an activity presents a prima facie case of circumvention is implicit in the Office's rulemaking authority."[286] In cases where exemptions are obligatory, narrowing the analysis to facts directly relevant to the questions of circumvention and infringement would be in the Office's best interest.

What about considering a separate and alternate group? Given the importance of security research for the health and safety of our digital infrastructure, the DMCA must be governed in a manner that protects the rights of security researchers. Separate and impartial, consider an independent, multi-stakeholder organization. There are several reasons why an independent, multi-stakeholder organization is the best choice to govern the DMCA.[287] First and foremost, this type of organization would be able to bring together a wide range of perspectives and expertise, ensuring that the needs of security researchers are considered alongside the interests of other stakeholders, such as copyright holders and technology companies.[288]

Furthermore, an independent, multi-stakeholder organization would have the resources and expertise to conduct rigorous research and analysis of the impact of the DMCA on security research, as well as the ability to engage in informed and productive discussions with other stakeholders about how to balance the needs of security researchers with other interests.[289] This organization could also provide a platform for security researchers to voice their concerns and needs and to help develop best practices for conducting security research in a way that is both effective and compliant with the requirements of the DMCA. Moreover, the independent, multi-stakeholder organization's advantages are its likelihood of being more transparent and accountable than a government-led entity. For example, a government-led organization might be swayed by political considerations or be

283. Perzanowski, *supra* note 278.

284. *See* USCO Letters to Other Agencies, U.S. COPYRIGHT OFFICE, https://www.copyright.gov/1201/2015/USCO-letters/ (last visited Jan. 14, 2023) [https://perma.cc/27G3-RJZY].

285. In a letter to the Office, the National Telecommunications and Information ("NITA") noted the "extensive discussion of matters with no or at best a very tenuous nexus to copyright protection," NTIA urged the Office to avoid "interpreting the statute in a way that would require it to develop expertise in every area of policy that participants may cite on the record." Letter from Lawrence E. Strickling, Assistant Sec'y. for Commc'ns & Info. & Adm'r of Nat'l Telecomm. & Info. Admin., to Maria A. Pallante, Register of Copyrights 3–4 (Sept. 18, 2015), https://copyright.gov/1201/2015/2015_NTIA_Letter.pdf [https://perma.cc/44SC-VQ9Z].

286. *Id*.; *see* 17 U.S.C. § 1201(a)(1)(C).

287. Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum*, UNITEDDIVERSITY (May 9, 2008) https://library.uniteddiversity.coop/Cooperatives/Multi-Stakeholder_Co-ops/Multi-Stakeholder_Governance_And_The_Internet_Governance_Forum.pdf [https://perma.cc/JH83-4Z7P].

288. Daniel Berliner et al., *Process Effects of Multistakeholder Institutions: Theory and Evidence From the Open Government Partnership*, 16 REGULATION & GOVERNANCE, JOHN WILEY & SONS 1343-1361 (2021).

289. *Cybersecurity Policy Making at a Turning Point*, OECD (Mar. 21, 2012) https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [https://perma.cc/LE24-63UE].

subject to pressure from certain interest groups. Alternatively, an independent organization would be more likely to make decisions in the best interests of security researchers and the public. "Many strategies share the view that dialogue with non-governmental stakeholders is key to good cybersecurity policy making and implementation. . . . In general, input from business is widely recogni[z]ed as essential, including for the implementation of the strategies. . . ."[290]

Therefore, an independent, multi-stakeholder organization is the best entity to protect the rights and interests of security researchers, as it would bring together a wide range of perspectives and expertise, provide a platform for security researchers to voice their concerns, and be more transparent and accountable than a government-led entity. The health and safety of our digital infrastructure depend on the ability of security researchers to do their work, and the DMCA must be governed in a manner that supports, rather than hinders, their efforts.[291]

VII. CONCLUSION

As illustrated, cybersecurity is a crucial aspect of our daily lives. With the modern person carrying around, in their pocket, a device that has more computing power than all the greatest computers throughout the turn of the 21st century, it is reasonable that we concern ourselves with ways to secure devices that could pose harm to life, livelihood, and national security. But importantly, as we have seen, the DMCA is not one of those ways.

Section 1201 of the DMCA is a provision that, unfortunately, harms security researchers and the security of our online systems and networks. Instead of incentivizing ethical hacking and promoting online security, Section 1201 creates a hostile legal environment for security researchers. Under Section 1201, security researchers who engage in good-faith testing computer systems and networks can be liable for copyright infringement if they inadvertently discover copyrighted material during their investigations. This creates a significant disincentive for security researchers to engage in ethical hacking, as they risk facing legal consequences for their work.

Moreover, Section 1201 stifles innovation and creativity in cybersecurity, as security researchers cannot freely explore and report security vulnerabilities without fear of legal repercussions. So, potential security threats are addressed, and the public is left vulnerable to cyber-attacks. In light of these concerns, it is clear that Section 1201 of the DMCA needs to be reformed. We need to create a legal

290. *Id*.

291. The Copyright Office is a department within the Library of Congress responsible for registering copyrights, providing information and guidance on copyright law, and advising Congress on national and international copyright issues. Under Article 1 of the U.S. Constitution, the Copyright Office is part of the legislative branch of government and is responsible for executing copyright laws. So, in addition and in support of the suggestions, some ways the Copyright Office could be reshaped include: (1) Modernizing systems and processes. The Copyright Office could be updated to adopt modern technologies and processes to improve efficiency, accuracy, and speed. This could include implementing electronic systems for registering copyrights, searching records, and communicating with copyright holders and users. (2) Increasing transparency and accountability. The Copyright Office could be reshaped to increase transparency and accountability by providing more information about its operations, processes, and decision-making. (3) Introducing greater independence to the Library. The Copyright Office could be given greater independence from the Library of Congress and other government agencies to ensure it can carry out its mission without undue influence or interference. (4) Expanding the role of the Office. The Copyright Office could include new responsibilities, such as providing education and training on copyright law and mediating disputes between copyright holders and users.

environment that supports ethical hacking and promotes online security rather than one that hinders it. By reforming Section 1201, we can ensure that security researchers can perform their work effectively and that the public is protected against malicious cyber-attacks.

The current technological climate calls for improved reliability and guidance regarding existing legal authorities, as well as how investigations should be held concerning security research. In addition, researchers are increasingly becoming independent and no longer affiliating themselves with institutions that housed them in the past (such as universities). This means they are moving away from restrictive research houses and opening to the public about vulnerabilities that would have previously been prohibited under contract—limiting those who can bring claims against researchers. Significantly, this is affecting the way inexperienced vendors go about handling reports.

Vulnerability reports are invaluable to the overall climate of security research. Safe harbors for researchers who use permissible procedures would resolve the tensions between researchers and vendors. Although it may be challenging to come to an amicable agreement, it is better than the alternative—keeping the uninformed vendor unaware of the threats from malicious hackers taking advantage of companies and their products without security researchers protecting them.

Although there has been a steady growth in the development of the DMCA's 1201 anti-circumvention exemptions, there remains a void of uncertainty regarding what will happen within the next three years. Until then, steps should be taken and implemented to expand cybersecurity's protective reach. Enabling security research is, therefore, the first step. Devices save countless lives every day; nevertheless, manufacturers may lack a fully competent level of cybersecurity engineering and a complete understanding of how a compromised device they manufacture can negatively affect organizations and individuals. The result: device manufacturers respond with hostility when first encountering a security researcher pointing out security flaws in their devices. The connection between security research and certain consumer products is where most of this argument lays its foundation. Public awareness of the benefits of security research will improve policy decisions, providing further understanding of contributions made to digital safety and security.

The legal system must do more to make designations between benevolent and malicious hackers to reduce the current conflation between the two. Broad interpretations of the 'anti-hacking" laws create less secure networks and the degree of uncertainty increases. Tailoring those who regulate the DMCA by engaging industry experts well-equipped for this function would take the burden away from uninformed lawmakers (who may not fully comprehend the security industry and what is technologically involved in secure device manufacturing). That is not to say it should be regulated by industry experts wholly disconnected from the legal world. Instead, the proposal is that because the digital age moves at a pace far quicker than the law can keep up with, security and software experts are the only ones who know how to approach change in this world well enough to make a positive impact. Therefore, I argue they should have a solid presence at the decision-making table.

Via the creation of a permanent anti-circumvention exception, or an entirely new law, security researchers will be able to (legally) support companies. Without such ambiguity in DMCA Section 1201, researchers will report glitches, flaws, and vulnerabilities to manufacturers or through legal channels and freely help protect consumers, patients, and others while improving the device manufacturing process.