Brooklyn Law Review

Volume 83 | Issue 4 Article 3

7-20-2018

No Security Through Obscurity: Changing Circumvention Law to Protect our Democracy Against Cyberattacks

Andrew Moshirnia

No Security Through Obscurity

CHANGING CIRCUMVENTION LAW TO PROTECT OUR DEMOCRACY AGAINST CYBERATTACKS

Andrew Moshirnia[†]

INTRODUCTION

In just the span of a year, Russian cyberattacks fundamentally undermined the electoral process of the United States and plunged Ukraine into darkness, twice.[1] Not to be outdone, as yet unidentified foreign hackers launched ransomware[2] that threatened to cripple hospitals around the globe.[3] It is thus beyond question that 2016 was the most dangerous year to date for cyberattacks against our critical national infrastructure. Yet, little attention has been paid to laws hindering our ability to defend ourselves. In fact, our own intellectual property law regime has constrained our ability to prepare for and thwart these attacks.

To date, the problem of national security has been largely ignored in the intellectual property law regime. Indeed, the scant attention of state actors has been primarily devoted to blocking potentially dangerous information from entering

---

† Senior Lecturer, Monash Business School, Monash University; Empirical IP Fellow, Chicago-Kent College of Law. The author would like to thank Ashley Chung, Fanxi Wang, Aaron Dozeman, Brian Sheppard, Hank Greenberg, and Rachel Capata for their assistance.

1 *See infra* Sections I.A–B.

2 Ransomware encrypts data on a machine and ransoms the data back to the user by way of decryption. Ransomware has become more prevalent in the last two years, with fairly popular programs such as CryptXXX, CTB-Locker, and Cerber. Lawrence Abrams, *The Cerber Ransomware Not Only Encrypts Your Data but Also Speaks to You*, BLEEPING COMPUTER (Mar. 3, 2016, 6:09 PM), https://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/ [https://perma.cc/83MB-RVJ3]; Caleb Fenton, *New CryptXXX Variant Discovered*, SENTINELONE (June 27, 2016), https://sentinelone.com/blogs/new-cryptxxx-variant-discovered/ [https://perma.cc/4VX2-SEAK]; *The Current State of Ransomware: CTB-Locker*, SOPHOS NEWS (Dec. 31, 2015), https://blogs.sophos.com/2015/12/31/the-current-state-of-ransomware-ctb-locker/ [https://perma.cc/5N6W-Y28D].

3 *See infra* Section I.C.

the public sphere.[4] The conventional approach of effectuating national security through intellectual property secrecy is approximately a century old, evolving from temporarily suppressing patents during wartime to one of perpetual secrecy in the face of unending conflict. While employing "security through obscurity"[5] to hide system vulnerabilities may have limited success in select circumstances, the interconnected nature of digital infrastructure and the cyber-warfare it invites renders such an approach foolhardy and dangerous, and leaves security to chance.

This underlying approach has been co-opted by powerful rights holders, who may piggyback on the notion of security through secrecy to attain extra-legal rights in otherwise constrained fields, such as an independent anticircumvention right gifted in a purported copyright act.[6] Section 1201 of the Digital Millennium Copyright Act (DMCA) creates a wholly novel anticircumvention right that frustrates security and encryption

---

[4] These concerns have spanned atomic secrecy to biological research publications into "dual use" fields. *See* Invention Secrecy Act, 35 U.S.C. §§ 181, 186 (2000) (prohibiting disclosure of inventions, if the inventions have been ordered kept secret on the ground that revealing them would be "detrimental to the national security"); Atomic Energy Act, 42 U.S.C. §§ 2014, 2274 (2000) (prohibiting disclosure of certain data concerning nuclear weapons); United States v. Progressive, Inc., 486 F. Supp. 5 (W.D. Wis.) (enjoining the publication of an article on the false premise that it contained information on how a hydrogen bomb could be constructed), *appeal dismissed*, 610 F.2d 819 (7th Cir. 1979); NAT'L RESEARCH COUNCIL, SCIENCE AND SECURITY IN A POST 9/11 WORLD: A REPORT BASED ON REGIONAL DISCUSSIONS BETWEEN THE SCIENCE AND SECURITY COMMUNITIES 58 (2007) ("Although the risk that pathogens will be used for harm has been around for centuries, the emerging global, fast-paced, and collaborative nature of the life sciences now makes protecting information, personnel, and materials from abuse that much more difficult. To effectively identify dual-use research of concern, and perhaps restrict it, techniques must be available to determine what types of biological agents could stand as threats, as well as what types of mathematics, software programs, physical materials, and computational tools could enhance biological threats."); Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1222 (2005).

[5] This method relies on

> secrecy of design and implementation to achieve a feeling of security. A system relying on security through obscurity may have serious security vulnerabilities, while its owners and designers wish that simply by not informing others of the flaws, no attacker will find them. This approach only creates an illusion of security.

HARRI HURSTI, THE BLACK BOX REPORT: CRITICAL SECURITY ISSUES WITH DIEBOLD OPTICAL SCAN DESIGN 2 (2005), http://www.blackboxvoting.org/BBVreport.pdf [https://perma.cc/9MV8-JPE8]. The attack on this method of security dates back to 1853 in response to fears that publications regarding locks and safes would inspire a wave of lock-picks. "Rogues are very keen in their profession, and know already much more than we can teach them." Tal Klein, *The Tao of Responsible Disclosure*, WIRED (Oct. 2014), https://www.wired.com/insights/2014/10/the-tao-of-responsible-disclosure/ [https://perma.cc/4Q3A-57CB].

[6] *See infra* Part III.

researchers alike.[7] Though these expansions have correctly concerned consumers, researchers, and rights activists,[8] the fundamental tenet of the regime—secrecy enhances security—stubbornly endures.

This article illuminates the archaic and harmful secrecy-focused intellectual property approach and suggests a new course in the face of evolving national threats. Part I sets out the dire cyber-warfare climate. Part II explores the secrecy approach evolving from the Invention Secrecy Act involving patents during wartime to the Atomic Energy Act and anti-decryption export controls. Part III describes the anticircumvention provisions of the DMCA that inadvertently encourage a security through obscurity approach and serve to chill much of the same research targeted by unconstitutional export controls. Part IV proposes a security-strengthening "defense in depth" approach based on responsible openness tenets to leverage community research, improve network vitality, and combat cyber-threats. Part V addresses likely counterarguments and areas for further research.

I. GLOBAL CYBERATTACKS AND THE GROWING DEMAND FOR SECURITY RESEARCH

The spate of cyberattacks against vital infrastructure—electoral, nuclear, and medical—undertaken by foreign actors signals the need for greater defense in an era of constant electronic warfare. This Part details the most troubling of these recent attacks: the Russian-led attacks on the United States' 2016 Presidential election, Russian intrusions in energy sectors, and the (as-yet unsourced) Wannacry ransomware attack on the international medical system.

---

[7] *See infra* Section III.D.

[8] While there are compelling arguments couched in constitutional principles to do away with this provision, there has been a reluctance to examine the bedrock behind this entire doctrine—does intellectual property secrecy serve to buttress national security? The answer is clearly no. Moreover, a policy-based approach is necessary, as courts have shown a frightening willingness to contort constitutional law in the face of national security threats. *See* Andrew V. Moshirnia, *Valuing Speech and Open Source Intelligence in the Face of Judicial Deference*, 4 HARV. NAT'L SEC. J. 385, 411–14 (2013) (collecting wartime cases distorting First Amendment jurisprudence and noting that the Court deliberately misapplied strict scrutiny in *Holder v. Humanitarian Law Project*, 561 U.S. 1, 8 (2010)); *see also infra* Sections II.A–B (noting judicially enforced speech suppression and speech compulsion in matters of national security).

A. Russian Electoral Cyberattacks

Recent Russian cyberattacks against American electoral integrity have captured the public's attention.[9] The damage is still being uncovered,[10] but the coordinated effort involved at least three distinct avenues of intrusion, targeting: (1) voting machines; (2) the election systems of thirty-nine states; and (3) individual accounts of election participants, including the Democratic National Committee (DNC). The latter of these attacks is well-known, while the former two have received far less attention. The attribution of these attacks to Russia is strengthened by a pattern of similar attacks conducted by Russia against Ukraine.[11] Former FBI Director James Comey opined that the Russians are not done meddling: "They're coming after America. . . . [T]hey will be back."[12] The coordinated attack on the foundation of American democracy

---

[9] *See generally* U.S. DEP'T OF HOMELAND SEC. & FED. BUREAU OF INVESTIGATION, JAR-16-20296A, NCCIC JOINT ANALYSIS REPORT: GRIZZLY STEPPE—RUSSIAN MALICIOUS CYBER ACTIVITY (Dec. 29, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf [https://perma.cc/689F-VM95] (detailing Russian interference in the 2016 presidential election). America is not the only country experiencing Russian electoral meddling. *See* Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (Jan. 9, 2017, 8:01 AM ET), http://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/ [https://perma.cc/GY32-J88G] ("Cyberattacks in Ukraine, Bulgaria, Estonia, Germany, France and Austria that investigators attributed to suspected Russian hackers appeared aimed at influencing election results, sowing discord and undermining faith in public institutions that included government agencies.").

[10] Jessica Taylor, *Source: Mueller Using D.C. Grand Jury in Russia Probe*, NAT'L PUB. RADIO (Aug. 3. 2017), http://www.npr.org/2017/08/03/541432868/source-mueller-using-d-c-grand-jury-in-russia-probe [https://perma.cc/MV8D-MXRB] (detailing Special Counsel Robert Mueller's "investigation into Russian efforts to influence the 2016 presidential election and into possible collusion between Russia and top aides to the Trump campaign").

[11] *See infra* Section I.A.4.

[12] 163 CONG. REC. S3480 (daily ed. June 14, 2017) (statement of Sen. Durbin), https://www.congress.gov/congressional-record/2017/6/14/senate-section/article/s3462-3 [https://perma.cc/GF3C-LPAX]; *see also Full Text: James Comey Testimony Transcript on Trump and Russia*, POLITICO (June 8, 2017, 1:48 PM EDT), http://www.politico.com/story/2017/06/08/full-text-james-comey-trump-russia-testimony-239295 [https://perma.cc/SZU3-82JR] (noting the bipartisan importance of a full investigation into Russian electoral meddling: "It is not a Republican thing or a democratic thing. It really is an American thing. They're going to come for whatever party they choose to try and work on behalf of, and they're not devoted to either, in my experience. They're just about their own advantage. They will be back."); *Full Transcript: FBI Director James Comey Testifies on Russian Interference in 2016 Election*, WASH. POST (Mar. 20, 2017), https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.8b0123e11b37 [https://perma.cc/Z5Q2-CLG4].

highlights the existential threat of such attacks and the importance of improving cybersecurity.[13]

1. Voting Machines

Electronic voter machines have long been flagged as a weak spot in electoral infrastructure,[14] as they present security,[15] logistical,[16] and financial[17] challenges. These difficulties are

---

[13] Former Director of National Intelligence James Clapper warned, "An American citizen should be very concerned about a foreign government, particularly our primary adversary, interfering with the most important foundational process that we have in this country, which is free and fair elections." Mallory Shelbourne, *Clapper: 'Aggressiveness' of Russian Interference in Election 'Unprecedented'*, HILL (May 30, 2017, 8:22 AM EDT), http://thehill.com/homenews/news/335575-clapper-aggressiveness-of-russian-interference-in-election-unprecedented [https://perma.cc/T7RW-KCFA].

[14] *See, e.g.*, Bruce Schneier, *The Problem with Electronic Voting Machines*, SCHNEIER ON SECURITY (Nov. 10, 2004), https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html [https://perma.cc/N2NW-YBN2] (collecting known voting machine malfunctions, including: "Fairfax County, VA, in 2003, a programming error in the electronic voting machines caused them to mysteriously subtract 100 votes from one particular candidates' totals. In San Bernardino County, CA in 2001, a programming error caused the computer to look for votes in the wrong portion of the ballot in 33 local elections, which meant that no votes registered on those ballots for that election. A recount was done by hand. In Volusia County, FL in 2000, an electronic voting machine gave Al Gore a final vote count of negative 16,022 votes. The 2003 election in Boone County, IA, had the electronic vote-counting equipment showing that more than 140,000 votes had been cast in the Nov. 4 municipal elections. The county has only 50,000 residents and less than half of them were eligible to vote in this election."); HACKING DEMOCRACY (Home Box Office 2006), http://www.hackingdemocracy.com/ [https://perma.cc/N7DF-G5EH] (Emmy-nominated documentary of flawed security of Diebold Election Systems, including the famous "Hursti Hack" in which Harri Hursti's team successfully altered votes on a Diebold voting machine); HURSTI, *supra* note 5.

[15] *Voting System Security and Reliability Risks*, BRENNAN CTR. FOR JUSTICE (2016), https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf [https://perma.cc/8Z39-SP7V].

[16] Lawrence Norden & Christopher Famighetti, *America's Voting Technology Crisis*, ATLANTIC (Sept. 15, 2015), https://www.theatlantic.com/politics/archive/2015/09/americas-voting-technology-crisis/405262/ [https://perma.cc/6879-JY6K] (noting that a large number of voting machines are at the end of their lifespan. "[F]or machines purchased since 2000, the expected lifespan for the core components of electronic voting machines is generally between [ten] and [fifteen] years. The majority of machines in use in the United States are perilously close to or exceed these estimates. In [forty-three] states, the oldest machines will be at least [ten] years old next November. In [fourteen] states they will be more than [fifteen] years old."); Lauren Smiley, *America's Voting Machines Are a Disaster in the Making*, NEW REPUBLIC (Oct. 19, 2016), https://newrepublic.com/article/137115/americas-voting-machines-disaster-making [https://perma.cc/RDD3-QY8C] (noting that one expert "fears faulty machines more than foreign hackers. A buggy voting machine, for example, could cause long lines at the polls in a crucial swing state, or a faulty touch-screen could switch votes from Trump to Clinton. And even if such glitches don't affect the outcome of the election, a snafu or two in traditional GOP strongholds will most definitely fuel the conspiracy theories").

[17] Congress initially financed the move to electronic voting machines as a result of the difficulty of the 2000 Election recount. The passage of the Help America Vote Act in 2002 set aside $4 billion to replace old punch card machines associated with the "dimpled chad" debacle. *See* Jaeah Lee, *Digital Voting Machines: Still*

heightened in the cases of voting machines that do not produce a paper record that can be reviewed or audited, allowing an intrusion or error to go undetected, absent a statistical audit.[18] This problem is not limited to a few jurisdictions—fourteen states use machines that produce no records, with five of those states relying on "paperless electronic voting machines as their primary polling place equipment statewide."[19] While there has been coverage of voting machines' technical issues across states on election day,[20] there has been comparatively little media coverage of a greater calamity[21]: a Russian effort to infiltrate machine manufacturers and potentially manipulate votes.[22]

According to a top-secret National Security Agency (NSA) report:

FUBAR??, MOTHER JONES (Nov. 6, 2012), http://www.motherjones.com/politics/2012/07/digital-voting-machines-fail-hacked/ [https://perma.cc/UJX6-BY88]; Jessica Reeves, *The Dimpled Chad Dilemma*, TIME (Nov. 21, 2000), http://content.time.com/time/nation/article/0,8599,89086,00.html [https://perma.cc/7P8V-3JKN]. Whereas mechanical systems may be built to last decades, electronic machines have a shorter lifespan. The amount of money needed to replace obsolete voting machines is estimated to be $1 billion. Norden & Famighetti, *supra* note 16. Moreover, Congress has shown little inclination to help meet this challenge, as voting machine purchases are typically treated as local issues. *See* Pam Fessler, *Voting Machines Are Aging, but Don't Expect Congress to Pay to Replace Them*, NAT'L PUB. RADIO (Oct. 11, 2015, 11:46 AM ET), http://www.npr.org/sections/itsallpolitics/2015/10/15/448931114/voting-machines-are-aging-but-dont-expect-congress-to-pay-to-replace-them [https://perma.cc/N89T-VBWU]; J.B. Wogan, *Voting Technology Needs an Upgrade, but Who Will Pay for It?*, GOVERNING MAG. (Nov. 2016), http://www.governing.com/topics/elections/gov-voting-technology-machines.html [https://perma.cc/VZ4H-NV33].

[18] *See* AJ Vicens, *Trump Says the Election Will Be Rigged. In These States, It May Be Impossible to Prove Him Wrong*, MOTHER JONES (Aug. 9, 2016, 4:59 PM), http://www.motherjones.com/politics/2016/08/millions-voters-could-cast-ballots-machines-leave-no-paper-trail/ [https://perma.cc/U279-VE9M] (noting that machines that leave no paper trail are particularly vulnerable to hacking).

[19] *Voting System Security and Reliability Risks*, *supra* note 15, at 2 n.3 (noting that "[i]n Arkansas, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas, and Virginia, some portion of polling places use such paperless machines as the primary equipment").

[20] *See, e.g.*, Charlotte Alter, *Detroit Voting Machine Failures Were Widespread on Election Day*, TIME (Dec. 14, 2016), http://time.com/4599886/detroit-voting-machine-failures-were-widespread-on-election-day/ [https://perma.cc/P8P9-MGQ8]; Mark Berman, Sari Horwitz & William Wan, *Voters Encounter Some Malfunctioning Machines, Other Headaches on Election Day*, WASH. POST (Nov. 8, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/11/08/election-day-voters-report-long-lines-intimidation-and-confusion-in-some-parts-of-the-country/ [https://perma.cc/76MU-XEKM].

[21] This may be due in part to the Department of Homeland Security's refusal to fully investigate the matter. *See* Sam Thielman, *The DHS Hasn't Investigated Whether Voting Machines Were Hacked in November, and Says It Doesn't Intend To*, BUSINESS INSIDER (June 30, 2017, 10:11 AM), http://www.businessinsider.com/dhs-is-refusing-to-investigate-hack-of-voting-machines-2017-6 [https://perma.cc/UFK7-EEA8].

[22] Nicole Perlroth, Michael Wines & Matthew Rosenberg, *Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny*, N. Y. TIMES (Sept. 1, 2017), https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html? [https://perma.cc/LP9V-ZKH2].

> Russian General Staff Main Intelligence Directorate actors . . . executed cyber espionage operations against a named U.S. company in August 2016, evidently to obtain information on elections-related software and hardware solutions. . . . The actors likely used data obtained from that operation to . . . launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations.[23]

Spear-phishing emails, targeted emails delivering compromising malware, were sent to seven employees of VR Systems, an electronic voting services and equipment provider for eight states.[24] At least one of those potential victims appears to have been compromised.[25]

Using the login credentials gathered from that initial attack, hackers started a second phase of sending targeted emails to local election officials under the guise of VR Systems.[26] These emails contained a Word document that purported to be system documentation for VR's product line, but which actually was a piece of malware created to hijack the target computer and force the download of a second malware bundle. It is still unclear if this phase of the attack was successful.[27]

While there is no evidence that Russian hackers sought to reassign votes, such an attack is technically possible. Alex Halderman, coincidentally one of the most prominent researchers chilled in a frivolous DMCA action,[28] noted: "So as

---

[23] Matthew Cole, Richard Esposito, Sam Biddle & Ryan Grim, *Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election*, INTERCEPT (June 5, 2017, 3:44 PM), https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ [https://perma.cc/H4CG-J5B4].

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Halderman discovered that an invasive Digital Rights Management (DRM) program embedded in music CDs could be disabled simply by pressing down the shift key when the disc was loading. His discovery caused the DRM manufacturer to experience a twenty-five percent drop in stock price and precipitated a threat of suit under the DMCA. *See* Katie Dean, *Shift-Key Case Rouses DMCA Foes*, WIRED (Oct. 11, 2003, 2:00 AM), https://www.wired.com/2003/10/shift-key-case-rouses-dmca-foes/ [https://perma.cc/9ULT-AQC2]; *see also Student Who Revealed CD Copying Secret Could Be Sued*, CNN (Oct. 13, 2003, 5:32 PM EDT), http://www.cnn.com/2003/TECH/biztech/10/10/bmg.protection.reut/ [https://perma.cc/XW5E-NEEP]. The company initially reveled in the power of the DMCA, stating, "This cat-and-mouse game that hackers and others like to play with owners of digital property is over. No matter what their credentials or rationale, it is wrong to use one's knowledge and the cover of academia to facilitate piracy and theft of digital property."
SunnComm CEO Says Princeton Report Critical of its MediaMax CD Copy Management Technology Contains Erroneous Assumptions and Conclusions, BUSINESS WIRE (Oct. 9, 2003, 1:38 PM EDT), http://www.businesswire.com/news/home/20031009005573/en/SunnComm-CEO-Princeton-Report-Critical-MediaMax-CD [https://perma.cc/FJV8-GPKV]. The company backed down in the face of

a remote attacker, I can target an election management system, one of these ballot programming computers. If I can infect it with malicious software, I can have that malicious software spread to the individual machines on the memory cards, and then change votes on Election Day."[29] This threat is all too real, as Russian-aligned hackers have previously attempted to change vote tallies in corrupted machines.[30]

2. State Election Offices

Russian hackers also targeted the election rolls, successfully breaching systems in thirty-nine states. In Illinois, cyber-intruders attempted to delete and alter voter data; according to the general counsel for the Illinois Board of Elections, in 2016 a contractor detected a breach.

The hackers had gained access to the state's voter database, which contained information such as names, dates of birth, genders, driver's licenses and partial Social Security numbers of 15 million people, half of whom were active voters. As many as 90,000 records were ultimately compromised.[31]

Russian attacks were widespread. "Thirty-seven states reported finding traces of the hackers in various systems, according to one of the people familiar with the probe. In two others—Florida and California—those traces were found in systems run by a private contractor managing critical election systems."[32]

---

widespread ridicule. *See* Lisa Napoli, *Compressed Data; Shift Key Opens Door To CD and Criticism*, N.Y. TIMES (Oct. 13, 2003), http://www.nytimes.com/2003/10/13/business/compressed-data-shift-key-opens-door-to-cd-and-criticism.html [https://perma.cc/2DT6-FH3M] (noting that the company dropped the threat of suit after receiving "three thousand e-mails").

[29] Pam Fessler, *If Voting Machines Were Hacked, Would Anyone Know?*, NAT'L PUB. RADIO (June 14, 2017, 5:00 AM ET), http://www.npr.org/2017/06/14/532824432/if-voting-machines-were-hacked-would-anyone-know [https://perma.cc/7H3M-YDF3]; Cole et al., *supra* note 23. It should be noted that the federal contractor that leaked the classified NSA report on this attack was soon thereafter arrested and charged with removing classified material. David Smith & Jon Swaine, *Russian Agents Hacked US Voting System Manufacturer before US Election*, GUARDIAN (June 5, 2017, 18:47 EDT), https://www.theguardian.com/technology/2017/jun/05/russia-us-election-hack-voting-system-nsa-report [https://perma.cc/Q3S3-2KSP]. This may have distracted the public at large from the content of the underlying report.

[30] *See infra* Section I.A.4.

[31] Michael Riley & Jordan Robertson, *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, BLOOMBERG (June 13, 2017, 5:00 AM EDT), https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections [https://perma.cc/96T5-XRTX].

[32] *Id.*

Security researchers have noted that voter registration databases "were never built with this kind of a threat in mind."[33] Indeed, Georgia's election system is so unguarded and reliant on off-the-shelf software that "a savvy 15-year-old hacker" could penetrate it.[34] Moreover, the disruption of this voter information on election day would be disastrous. "Dan Wallach, a computer security scholar at Rice University who recently testified in Congress about election system vulnerabilities noted, 'If I can destroy voting registration data, it does not matter how good the rest of your system is. You will have lines and a giant mess when people turn up to vote.'"[35]

This sort of attack is not far-fetched. There is strong evidence that the Obama Administration feared that it might come to pass in an effort "to undermine public faith in the U.S. democratic process."[36] The Administration drafted a contingency plan allowing for the deployment of "armed. . . . law enforcement agents" if Russian hackers succeeded in stopping voting.[37] Moreover, the plan included a three-day window to address "post-election cyber incidents" such as false news stories disputing the results.[38]

3. Democratic National Committee

The Russian attack that gained the most media attention was the coordinated effort to hack and leak internal emails related to the DNC and Democratic presidential nominee Hillary Clinton. While the investigation into possible collusion by U. S. citizens is ongoing, the underlying hacking effort is fairly well understood. The U.S. Intelligence Community concluded,

> The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. [They] assess[ed] that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party

---

[33] Evan Halper, *U.S. Elections Are an Easier Target for Russian Hackers Than Once Thought*, L.A. TIMES (July 28, 2017), http://www.latimes.com/politics/la-na-pol-elections-hacking-2017-story.html [https://perma.cc/X6AY-KQTR].

[34] *Id.*

[35] *Id.*

[36] Massimo Calabresi, *Exclusive: Read the Previously Undisclosed Plan to Counter Russian Hacking on Election Day*, TIME (July 20, 2017), http://time.com/4865798/russia-hacking-election-day-obama-plan/ [https://perma.cc/VWA5-TZAC].

[37] *Id.*

[38] *Id; see also* Shimon Prokupecz, Pamela Brown & Evan Perez, *Exclusive: FBI Tracked 'Fake News' Believed to Be from Russia on Election Day*, CNN (Aug. 4, 2017, 4:33 PM ET), http://www.cnn.com/2017/08/04/politics/election-day-cyber-threat-fbi-monitoring/index.html [https://perma.cc/6RHE-XW6J] ("'We were right on the edge of Constitutional legality,' a person briefed on the investigation said. 'We were monitoring news.'") (internal quotation marks omitted).

> officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.[39]

Russian hacker Guccifer 2.0,[40] potentially with the assistance of GOP-connected go-betweens,[41] sorted the materials and selectively leaked them to Wikileaks, which then released the information in batches to the press.[42]

4. Prior Election Cyberattacks by Russia

The intelligence community's attribution of the attacks to Russia is strengthened by Russia's prior election cyberattacks in Ukraine.[43] In 2014[44] and again in 2015, the pro-

---

[39] NAT'L INTELLIGENCE COUNCIL, ICA 2017-01D, INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 2 (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/AZ2R-36MB].

[40] AJ Vicens, *DNC Hacker Dumps Trove of Clinton Documents: Guccifer 2.0 Strikes Again*, MOTHER JONES (June 21, 2016, 7:24 PM), http://www.motherjones.com/politics/2016/06/hacker-releases-another-set-dnc-documents-hillary-clinton/ [https://perma.cc/TKH9-3LHN]; Lorenzo Franceshi-Bicchierai, *'Guccifer 2.0' Is Likely a Russian Government Attempt to Cover Up Its Own Hack*, MOTHERBOARD (June 16, 2016, 1:35 PM), https://motherboard.vice.com/en_us/article/wnxgwq/guccifer-20-is-likely-a-russian-government-attempt-to-cover-up-their-own-hack [https://perma.cc/D4NX-SQJH].

[41] Alexandra Berzon & Rob Barry, *How Alleged Russian Hacker Teamed Up with Florida GOP Operative*, WALL ST. J. (May 25, 2017, 11:33 PM ET), https://www.wsj.com/articles/how-alleged-russian-hacker-teamed-up-with-florida-gop-operative-1495724787 [https://perma.cc/88W6-PWQG].

[42] *See, e.g.*, Dylan Byers, *Donna Brazile Out at CNN Amid Leaks to Clinton Campaign*, CNN MONEY (Oct. 31, 2016, 1:33 PM ET), http://money.cnn.com/2016/10/31/media/donna-brazile-cnn-resignation/ [https://perma.cc/ TDW8-7HD7].

[43] It should be noted that Ukraine is not the only former Soviet state that has experienced a wave of Russian cyberattacks. Estonia was the target of a two-week long cyberattack. Joshua Davis, *Hackers Take Down the Most Wired Country*, WIRED (Aug. 21, 2007, 12:00 PM), https://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all [https://perma.cc/N87L-W3EL] ("All major commercial banks, telcos, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation."); Scheherazade Rehman, *Estonia's Lessons in Cyberwarfare*, U.S. NEWS & WORLD REP. (Jan. 14, 2013, 3:34 PM), http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare ("Estonia shouted loudly from the roof tops that they were being attacked, that an act of war had being [sic] committed by the Russians, and called upon its allies to assist, but they had a hard time getting anyone to believe that this was a 'real war' and not a cybernuisance. In the end no one came to help the Estonians but what that alarm did do was to put global cyberattacks on the warfare discussion table for . . . NATO."). Bulgaria, a country that was once a member of the Warsaw Pact, also experienced major cyberattacks on election day. *See Bulgaria Will Leave Warsaw Pact, President Declares*, L.A. TIMES (Feb. 2, 1991), http://articles.latimes.com/1991-02-02/news/mn-395_1_warsaw-pact [https://perma.cc/6YUY-7N7L]; Gordon Corera, *Bulgaria Warns of Russian Attempts to Divide Europe*, BBC (Nov. 4, 2016), http://www.bbc.com/news/world-europe-37867591 [https://perma.cc/WGU9-CJV9] (noting a "denial of service attack—which tries to make websites inaccessible—targeted the electoral commission, presidency and other government institutions on the day of a referendum and local elections" that was considered "an attack

Russian hacktivist group CyberBerkut launched a series of distributed denial of service (DDoS) and other cyberattacks in an attempt to disrupt and discredit Ukrainian elections.[45] In May 2014, hackers infiltrated Ukraine's Central Election Commission (CEC) as a precursor to changing votes.[46] A mere forty minutes before results were to be announced on television, the Security Service of Ukraine (Sluzhba Bezpeky Ukrayiny or SBU) discovered a virus and removed it from the CEC's computers.[47]

> If it had not been discovered and removed, the malicious software would have portrayed ultra-nationalist Right Sector party leader Dmytro Yarosh as the winner with 37 percent of the vote (instead of the 1 percent he actually received) and Petro Poroshenko (the actually [sic] winner with a majority of the vote) with just 29 percent, Ukraine officials told reporters the next morning. Curiously, Russian Channel One aired a bulletin that evening declaring Mr. Yarosh the victor with 37 percent of the vote over Mr. Poroshenko with 29 percent.[48]

Russian efforts were not limited to targeted vote changing and also included a campaign to hinder vote counting and efficient result reporting. "[C]omputers of Ukraine's national election commission were hit with a major attack that deleted backups, damaged hard drives, make [sic] software unusable and changed routers settings."[49]

> In the wee hours of the morning after polls closed, as results flowed in from Ukrainian election districts, Internet links feeding that data to the vote tally system were hit with a barrage of fake data packets—known as distributed denial of service (DDoS) attacks. So from about 1 to 3 a.m. on May 26, election results were blocked,

---

on the Bulgarian state and the Bulgarian democracy and [was] conducted with a high probability from Russia") (internal quotation marks omitted).

[44] Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers*, CHRISTIAN SCI. MONITOR (June 17, 2014), http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video [https://perma.cc/YUP5-Z4YW].

[45] Margaret Coker & Paul Sonne, *Ukraine: Cyberwar's Hottest Front*, WALL ST. J. (Nov. 9, 2015, 9:14 PM ET), http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671 [https://perma.cc/Q4TV-RTP2].

[46] Katya Gorchinskaya, Olga Rudenko & William Schreiber, *Authorities: Hackers Foiled in Bid to Rig Ukraine Presidential Election Results*, KYIV POST (May 25, 2014, 7:47 PM), https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html [https://perma.cc/49NW-A73G].

[47] Clayton, *supra* note 44; Halya Coynash, *Russian Fake Shows CEC Claiming Right Sector Win*, HUMAN RIGHTS IN UKRAINE (May 26, 2014), http://khpg.org/en/index.php?id=1401060238 [https://perma.cc/PD2D-D5V9].

[48] Clayton, *supra* note 44.

[49] Elizabeth Weise, *'Getting Twitchy': Election Threats Have Cyber Experts Worried*, USA TODAY (Nov. 5, 2016, 2:09 PM ET), http://www.usatoday.com/story/tech/news/2016/11/04/cyber-threats-election-2016-russia-clinton-trump-ukraine-hack-ddos-dyn-denial-of-service-attack/93249646/ [https://perma.cc/VE9L-Y8D4].

> delaying the finally [sic] tally until the early morning, a preliminary report by international election observers recounted.[50]

Russian efforts focused on elections and demonstrate the danger posed by insufficient security.

B. Russian Cyberattacks on Energy Infrastructure

Intrusions in the electric grid are also cause for alarm.[51] In May 2017, Russian hackers infiltrated the business systems of U.S. nuclear power plants and other companies in the energy sector in an effort to gather personnel data.[52] This data could be used for more targeted attempts to compromise infrastructure, including gathering emails, communications about designs, security audits, poorly secured passwords, and known issues.[53] Additionally, hacking groups can use compromised inboxes to send false emails delivering malware to segregated systems.[54] According to Greg

---

[50] Clayton, *supra* note 44.

[51] Hackers have repeatedly targeted the Department of Energy. Between 2010 and 2014, "hackers targeted DOE networks 1,131 times over the four-year span, successfully cracking the network 159 times." Corey Bennett, *Energy Dept. Hacked 150 Times in 4 Years*, HILL (Sept. 9, 2015, 5:09 EDT), http://thehill.com/policy/cybersecurity/253130-hackers-cracked-energy-department-150-times-over-four-years [https://perma.cc/SJ34-RM6A]. Investigations into breaches found a number of troubling practices, including:

> [p]ermitting systems to operate even though they were known to have critical and/or high risk security vulnerabilities. The Department had not taken appropriate action to remediate known vulnerabilities on its systems either through patching, system enhancements or upgrades. [The Department] fail[ed] to assign the appropriate level of urgency to replacing end-of-life systems.

U.S. DEP'T OF ENERGY OFF. OF INSPECTOR GEN. OFF. OF AUDITS AND INSPECTIONS, DOE/IG-0900, SPECIAL REPORT: THE DEPARTMENT OF ENERGY'S JULY 2013 CYBER SECURITY BREACH 2 (2013), https://energy.gov/sites/prod/files/2013/12/f5/IG-0900.pdf [https://perma.cc/5XCH-KH6A].

[52] *See* Nash Jenkins, *Feds: Russian Hackers Are Attacking U.S. Power Plants*, TIME (Mar. 16, 2018), http://time.com/5202774/russia-hacking-dhs-report-power/ [https://perma.cc/W729-8N9Z]; Nicole Perlroth, *Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say*, N.Y. TIMES (July 6, 2017), https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html [https://perma.cc/4RGH-BA5N].

[53] Sonam Sheth, *Hackers Breached a US Nuclear Power Plant's Network, and It Could Be a 'Big Danger'*, BUSINESS INSIDER (June 29, 2017, 9:36 AM), http://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6 [https://perma.cc/P3HZ-MWYB].

[54] Elisabeth Leamy & Sally Hawkins, *'Stranded Traveler' Scam Hacks Victims' Emails, Asks Their Contacts for Money*, ABC NEWS (July 13, 2012), http://abcnews.go.com/Technology/stranded-traveler-scam-hacks-victims-emails-asks-contacts/story?id=16774896 [https://perma.cc/R7R5-UUB4]; Steve Ragan, *FTC Spam Campaign Snares Thousands of Targeted Victims*, CSO DASHBOARD (Dec. 7, 2016, 2:37 PM PT), http://www.csoonline.com/article/3148148/security/ftc-spam-campaign-snares-thousands-of-targeted-victims.html [https://perma.cc/JER5-YZ67] (noting heightened danger of targeted spam that appears to be sent from a trusted sender).

Martin, an expert with cybersecurity firm Jask, information gathered in this fashion "can be used [by hackers] to set up for future, more damaging attacks just based on the proprietary information they're able to steal."[55] While the attack did not appear to compromise plant software, the specter of Russian interference in the energy sector has become all too familiar.[56]

Successful Russian targeting of electric systems has been previously documented. In December 2015, Russian hackers crippled Ukraine's electric grid.[57] On December 23, 2015, the computer systems of regional electricity distributor Kyivoblenegro were infiltrated, impacting the supervisory control and data acquisition (SCADA) system of the company.[58] The primary attack hijacked SCADA in an effort to open breakers, while coordinated telephone floods jammed customer support lines.[59] At the same time, workstations and internal servers were wiped to delay restoration efforts.[60] In turn, thirty substations were brought off-line for three hours.[61] This outage, coupled with three other attacks in quick succession on different electric distribution companies, resulted in approximately 225,000 people losing power for several hours. [62]

Shortly following the attack, the Ukrainian government claimed that Russian security services were responsible.[63] Indeed, Russian hacking groups have been outspoken in their support of the Russian occupation of Crimea.[64] This attribution

---

[55] Sheth, *supra* note 53.

[56] *See* James Conca, *Is Hacking Nuclear Power Plants Something We Should Be Afraid Of?*, FORBES (July 7, 2017, 6:00 AM), https://www.forbes.com/sites/jamesconca/2017/07/07/is-hacking-nuclear-power-plants-something-we-should-be-afraid-of/#6e808815dde8 [https://perma.cc/8NSZ-KNVL] (arguing that the threat of hacking a nuclear plant is low but that the hacking of the energy grid is of much greater concern).

[57] ELECTRONIC INFO. SHARING & ANALYSIS CTR., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID 1 (Mar. 18, 2016) [hereinafter E-ISAC Report], http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf [https://perma.cc/34FY-LYU7]; Jim Finkle, *U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage*, REUTERS (Jan. 7, 2016, 7:20 PM), https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108 [https://perma.cc/8UWA-AGLL]; Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [https://perma.cc/89AC-CVK4].

[58] E-ISAC Report, *supra* note 57, at 1.

[59] *Id.* at 13.

[60] *Id.* at 11, 12.

[61] *Id.* at 1.

[62] *Id.*

[63] *Id.*

[64] The year after targeting Ukraine, CyberBerkut launched similar attacks against German websites, urging "all people and government of Germany [sic] to stop financial and political support of criminal regime in Kiev, which unleashed a bloody

is credible, especially in light of previous Russian-linked cyberattacks on Ukrainian targets and subsequent attacks on the Ukrainian energy grid.[65]

Almost a year later, Kiev again went dark.[66] This time, the attack centered on a transmission facility rather than a distribution facility, and it coincided with attacks on the Ministry of Finance, the Pension Fund, and the Treasury.[67] Again, the malware responsible was attributed to Russia,[68] which was likely using Ukraine as a testing ground for power-grid cyberweapons.[69] Ukraine has continued to be attacked with novel malware, shutting down airports, factories, and banks.[70] The latest attack received greater Western media attention, as it factored into reduced earnings of numerous

---

civil war. We are CyberBerkut! We will not forget! We will not forgive!" Dennis Lynch, *Pro-Russian Hacker Group CyberBerkut Claims Attack on German Government Websites*, INT'L BUS. TIMES (Jan. 7, 2015, 9:10 AM), http://www.ibtimes.com/pro-russian-hacker-group-cyberberkut-claims-attack-german-government-websites-1775874 [https://perma.cc/623V-8XPC] (quoting *CyberBerkut Has Blocked German Chancellor and the Bundestag's Websites*, CYBER BERKUT, http://www.cyber-berkut.ru/en/index_02.php [https://perma.cc/4GES-SRCQ]).

[65] *Russia Behind Cyber-Attack, Says Ukraine's Security Service*, BBC NEWS (July 2, 2017), http://www.bbc.com/news/world-europe-40471310 [https://perma.cc/ER9D-C6AW].

[66] Andy Greenberg, '*Crash Override': The Malware That Took Down a Power Grid*, WIRED (June 12, 2017, 8:00 AM), https://www.wired.com/story/crash-override-malware [https://perma.cc/AHX2-R45U].

[67] *Education Ministry Website Is Under DdoS-Attacks*, 112.UA INFO. AGENCY (Dec. 26, 2016 2:12 PM), http://112.international/society/education-ministry-website-is-under-ddos-attacks-12465.html [https://perma.cc/N88Z-PSBD]; Vsevolod Nekrasov, *Ukraine Is Losing a Cyberwar: Hackers Attacked Public Treasury*, 112.UA INFO. AGENCY (Dec. 12, 2016 2:30 PM), http://112.international/article/ukraine-is-losing-a-cyberwar-hackers-attacked-public-treasury-11957.html [https://perma.cc/5MCN-LWWL].

[68] Joe Uchill, *Researchers Break Down Malware Likely Used in Ukraine Blackout*, HILL (June 12, 2017, 11:09 AM EDT), http://thehill.com/policy/cybersecurity/337404-researchers-break-down-malware-likely-used-in-ukraine-blackout [https://perma.cc/K78N-6MXJ]; *Ukraine Power Cut 'Was Cyber-Attack'*, BBC NEWS (Jan. 11, 2017), http://www.bbc.com/news/technology-38573074 [https://perma.cc/B3DA-YYKL].

[69] *Experts Suspect Russia Is Using Ukraine as a Cyberwar Testing Ground*, NPR (June 22, 2017, 1:14 PM ET), http://www.npr.org/2017/06/22/533951389/experts-suspect-russia-is-using-ukraine-as-a-cyberwar-testing-ground [https://perma.cc/58ZU-ULNX]; Deborah Haynes, *Russia Has Edge over Us in Battle, Army Admits*, TIMES (London) (Aug. 10, 2016, 12:01 AM), https://www.thetimes.co.uk/edition/news/russia-has-edge-over-us-in-battle-army-admits-tsl7j63f5 [http://perma.cc/BV6L-47Q3].

[70] Lizzie Dearden, *Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport Hit by Hackers*, INDEPENDENT (June 27, 2017, 1:04 BST), http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html [https://perma.cc/SL6A-JBGV]; Nolan Peterson, *Whose Cyberattack Brought Ukraine to a Shuddering Halt?*, NEWSWEEK (July 1, 2017, 12:20 AM), http://www.newsweek.com/nolan-peterson-whose-cyberattack-brought-ukraine-shuddering-halt-630500 [https://perma.cc/3LW7-M4WC]; Pavel Polityuk & Alessandra Prentice, *Ukrainian Banks, Electricity Firm Hit by Fresh Cyber Attack*, REUTERS (June 27, 2017, 8:26 AM), http://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ [https://perma.cc/H4JN-G8GT].

multinational firms.[71] The main attack used a modified Petya[72] ransomware[73] variant, itself an offshoot of a leaked NSA exploit[74]: EternalBlue.[75] Security experts have warned that this sort of attack is likely being readied as a threat against NATO members, including the United States.[76]

C. Chinese or North Korean WannaCry Cyberattack on Hospitals

Russia is not the only state actor responsible for wide-ranging cyberattacks. On May 12, 2017, the Chinese[77] or North

---

[71] Jim Finkle & Eric Auchard, *Corporate Profits to Take More Hits from Ukraine Cyber Attack*, REUTERS (Aug. 2, 2017), https://www.reuters.com/article/us-cyber-results-idUSKBN1AI2CQ [https://perma.cc/PFG8-VF88] (noting that Cadbury chocolate and FedEx reported material financial damage due to the "worm").

[72] Olivia Solon & Alex Hern, *'Petya' Ransomware Attack: What Is It and How Can It Be Stopped?*, GUARDIAN (June 28, 2017, 2:17 EDT), https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how [https://perma.cc/JJ9M-M2VZ].

[73] Petya is considered "the next step in ransomware evolution." Aliaksandr Trafimchuk, *Decrypting the Petya Ransomware*, CHECKPOINT BLOG (Apr. 11, 2016), https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/ [https://perma.cc/5YBM-AMQL].

[74] For clarity, a "vulnerability" is a flaw in a security measure. Vulnerabilities may be artifacts of software, hardware or the structure of a system, but may also be linked to behavioral or social patterns. Known software vulnerabilities are collected in the Common Vulnerabilities and Exposures (CVE) catalog. The hope is that when a vulnerability is communicated to a vendor, the vendor will apply a patch to remove the flaw. An "exploit" is a term

> commonly used to describe a software program that has been developed to attack an asset by taking advantage of a vulnerability. The objective of many exploits is to gain control over an asset. For example, a successful exploit of a database vulnerability can provide an attacker with the means to collect or *exfiltrate* all the records from that database. The successful use of exploits of this kind is called a *data breach*. Exploits are also developed to attack an operating system or application vulnerability to gain remote administrative or "run" privileges on a laptop or server.

Dave Piscitello, *Threats, Vulnerabilities and Exploits—Oh My!*, ICANN: BLOG (Aug. 10, 2015), https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my [https://perma.cc/9DL3-PQ4E]. In this case, a vulnerability denoted as CVE-2017-0144 was found in Microsoft Windows. The NSA developed an exploit of that vulnerability. *Microsoft Security Bulletin MS17-010-Critical: Security Update for Microsoft Windows SMB Server (4013389)*, MICROSOFT (Mar. 14, 2017), https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 [https://perma.cc/4BE6-YHEH]; Matt Burgess, *Everything You Need to Know About EternalBlue—The NSA Exploit Linked to Petya*, WIRED (June 28, 2017), http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch [https://perma.cc/2ZEJ-JA8L].

[75] Tod Beardsley, *Petya-Like Ransomware Explained*, RAPID7: BLOG (June 27, 2017), https://community.rapid7.com/community/infosec/blog/2017/06/27/petya-ransomware-explained [https://perma.cc/6SRX-5W5J].

[76] Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 06:00 AM), https://www.wired.com/story/russian-hackers-attack-ukraine/ [https://perma.cc/28KC-Y5QR].

[77] *WannaCry Ransom Notice Analysis Suggests Chinese Link*, BBC NEWS (May 29, 2017), http://www.bbc.com/news/technology-40085241 [https://perma.cc/532Y-

Korean[78] WannaCry ransomware infected roughly a quarter of a million machines in 150 countries[79] through an exploit of Window's Server Message Block, EternalBlue.[80] The exploit is believed to have originally been created by the NSA, and was leaked to the public by the hacking group, The Shadow Brokers.[81]

The attack infected medical devices and took down entire radiology departments.[82] The malware encrypted the contents of devices and demanded payment for decryption. Numerous device manufacturers released critical warnings about the spread of the virus, instructing hospitals to unplug vulnerable machines.[83] Of note was the attack's infiltration of

---

CJ3Q] *But see* Danny Palmer, *China on WannaCry: It Wasn't Us, Honest*, ZDNET (Jun 13, 2017 10:39 GMT), http://www.zdnet.com/article/china-on-wannacry-it-wasnt-us-honest/ [https://perma.cc/XV2R-7WC4] (noting that some firms attribute the attack to the Lazarus Group, a hacking group linked to North Korea).

[78] Gordon Corera, *NHS Cyber-Attack Was 'Launched from North Korea'*, BBC NEWS (June 16, 2017), http://www.bbc.com/news/technology-40297493 [https://perma.cc/7LN3-8L4Z]; Cara McGoogan, *WannaCry Cyber Hackers Linked to China Not North Korea, Experts Say*, TELEGRAPH (May 30, 2017 11:16 AM), http://www.telegraph.co.uk/technology/2017/05/30/wannacry-linked-chinese-hackers-not-north-korea-experts-say/ [https://perma.cc/ZVQ6-2VYD].

[79] Bill Chappell, *WannaCry Ransomware: What We Know Monday*, NAT'L PUB. RADIO (May 15, 2017, 2:31 PM ET), https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday [https://perma.cc/BQZ7-6N5D]; Elizabeth Dwoskin and Karla Adam, *More Than 150 Countries Affected by Massive Cyberattack, Europol Says*, WASH. POST (May 14, 2017), https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.adb6e94ca674 [https://perma.cc/5VL2-ASUS]. For a larger analysis of the infection rates of Petya and WannaCry, see DICK O'BRIEN, SYMANTEC, INTERNET SECURITY THREAT REPORT: RANSOMWARE 2017 AN ISTR SPECIAL REPORT (July 2017), https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf [https://perma.cc/3NEM-GZCP].

[80] Burgess, *supra* note 74.

[81] Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT ON THE ISSUES (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0000mpb068egqcqczh61fx32wtiui [https://perma.cc/T2PY-Y7HH]; *see also* April Glaser, *U.S. Hospitals Have Been Hit by The Global Ransomware Attack*, RECODE (June 27, 2017, 6:47 PM EDT), https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals [https://perma.cc/7C2H-93CR].

[82] Thomas Fox-Brewster, *Medical Devices Hit by Ransomware for the First Time in US Hospitals*, FORBES (May 17, 2017, 9:00 AM), https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#7d6b880425cf [https://perma.cc/NX97-U8FX].

[83] *See, e.g.*, *Committed to Proactively Addressing the Security Concerns of Our Customers*, PHILIPS HEALTHCARE, https://www.usa.philips.com/healthcare/about/customer-support/product-security [https://perma.cc/R5QK-Z4AC]; *Customer Information on WannaCry Malware for Siemens Healthineers Imaging and Diagnostics Products*, SIEMENS PRODUCTCERT (May 16, 2017), https://www.siemens.com/cert/pool/cert/siemens_security_bulletin_ssb-421479.pdf [https://perma.cc/A7YL-FGRJ]; *GE Healthcare Guidance on WannaCry Ransomware*, GE HEALTHCARE, http://www3.gehealthcare.com.sg/en-gb/support/security [https://perma.cc/758U-

the U.K.'s National Health Service, impacting roughly twenty percent of hospital-managing trusts, and even reaching several U.S. hospitals, which have continued to feel the effects of the attack even after initial patching.[84] The attack did not focus on the medical sector alone,[85] infecting Spanish telecoms, gas, and electric companies. The success of WannaCry also inspired similar attacks linked to the same vulnerability; indeed, Petya and NotPetya ransomware continue to impact U.S. hospitals.[86]

The initial WannaCry infection could have been much worse, but for the discovery of a "kill switch" by an altruistic third party—Marcus Hutchins.[87] Hutchins, a twenty-two year old security researcher, noted that the malware's propagation mechanism referenced an unregistered domain.[88] The worm would attempt to connect to the domain and upon that ping's failure, the worm's behavior would remain unchanged.[89] By registering the domain, Hutchins was able to disable the worm and stop the global spread.[90] Hutchins subsequently donated to charity his $10,000 reward for helping stop the attack.[91]

2MG2]; *Information Technology Advisory—"WannaCry" Ransomware*, BAYER IN RADIOLOGY (May 17, 2017), https://www.radiologysolutions.bayer.com/service/information-technology-advisory/ [https://perma.cc/XL3E-2BBK] ("Bayer is aware of ransomware ('WannaCry') that is exploiting vulnerabilities in Microsoft (MS) Windows. If a hospital's network is compromised by the malware attack, the virus can spread through the hospital's information technology (IT) network. In this event, Bayer's Windows-based devices that are connected to the network may be impacted.").

[84] Heather Landi, *HHS Notice: WannaCry Malware Continues to Impact U.S. Healthcare Orgs*, HEALTHCARE INFORMATICS (June 6, 2017), https://www.healthcare-informatics.com/news-item/cybersecurity/hhs-notice-wannacry-malware-continues-impact-us-healthcare-orgs [https://perma.cc/3NPQ-5X33] ("The virus can persist even on a machine that has been patched, however, the virus will not spread to a patched machine, but the attempt to scan can disrupt Windows operating systems when it executes. The particular effect varies according to the version of Windows on the device, HHS stated.").

[85] Corera, *supra* note 78 (noting the "attack was indiscriminate rather than targeted").

[86] *See* Lily Hay Newman, *Latest Ransomware Hackers Didn't Make WannaCry's Mistakes*, WIRED (June 27, 2017, 7:23 PM), https://www.wired.com/story/petya-ransomware-wannacry-mistakes/ [https://perma.cc/QHA3-8HQE]; *see also* Glaser, *supra* note 81.

[87] *How to Accidentally Stop a Global Cyber Attacks*, MALWARETECH (May 13, 2017), https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html [https://perma.cc/424V-DK6Q]; Newman, *supra* note 86.

[88] *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/8QWR-GNZK].

[89] *Id.*

[90] *Id.*

[91] Rob Price, *The 22-Year-Old Brit Who Stopped the Global Cyberattack Is Donating His $10,000 Reward to Charity*, BUSINESS INSIDER (May 16, 2017, 5:47 AM), http://www.businessinsider.com/malwaretech-donate-10000-wannacry-reward-charity-ransomware-2017-5 [https://perma.cc/D4AH-RSFM]. It should be noted that Hutchins was subsequently arrested in the United States on charges related to other malware.

II. IP SECRECY DOCTRINES ENABLE A SECURITY THROUGH OBSCURITY APPROACH

The current relationship between intellectual property (IP) and national security is founded on the belief that secrecy of the former will strengthen the latter. One challenge to overcome when discussing the role of intellectual property in the national security context is the meretricious argument that "loose lips . . . sink ships."[92] This approach is an outgrowth of the Invention Secrecy Act during the world wars and the subsequent Atomic Energy Act, with a sustained urgency beginning during the Cold War and continuing through the War on Terror. These laws, in turn, informed American export control laws, which demonstrated a clear enmity to encryption in particular.

This Part traces the development of the security through obscurity IP doctrine embodied by the Invention Secrecy Act and export controls. Both demonstrate a clear suspicion of disseminating decryption information. While the DMCA does not spring from the same concerns as the security through obscurity doctrine, it achieves many of the same outcomes: chilling the publication of potentially sensitive findings and delimiting public availability of decryption information. Recent attempts to expand secrecy to economically valuable patents and to buttress the DMCA with stronger export controls further highlight the links between the two schools of thought.

A. The Invention Secrecy Act and Atomic Energy Act

During World War I, the impact of technological development on warfare was acutely evident, raising the fear that "inventions which are of most use to the Government during a time of war are also those which would, if known, convey useful information to the enemy."[93] Congress passed invention secrecy as part of the Trading with the Enemy Act of

---

Andy Greenberg, *Hacker Who Stopped WannaCry Charged with Writing Banking Malware*, WIRED (Aug. 3, 2017, 3:40 PM), https://www.wired.com/story/wannacry-malwaretech-arrest/ [https://perma.cc/2GDJ-R79V].

[92] Attila Nagy, *The Best Operations Security Propaganda Posters from World War II*, GIZMODO (Aug. 27, 2015, 3:35 PM), http://gizmodo.com/the-best-operations-security-propaganda-posters-from-wo-1726361670 [https://perma.cc/5NRZ-XQPP] (collecting multiple examples of WWII posters encouraging silence, including "Silence Means Security").

[93] S. REP. NO. 65-119, at 1 (1917).

1917 (TWEA),[94] barring the publication of patents that could be detrimental to the war effort.[95] In doing so, the United States followed the lead of other Allied states, including the British and French.[96] The TWEA may also be thought of as a key development in American wartime export control. Unsurprisingly, patent suppression went unused during the interbellum.[97]

The resumption of European conflict during World War II prompted Congress to amend the TWEA in the Act of July 1, 1940.[98] While the amended act initially had a two-year window,[99] which was necessary in light of the fact that the United States had not actually joined the war, the TWEA was later amended to remain effective for the duration of the war.[100] The same year, Congress passed the Export Control Act (ECA), granting the President the authority to bar the export of munitions and aircraft supplies without a license.[101]

While the TWEA of 1917 and its amended form in 1940 contemplated only restrictions of IP in wartime or during national emergencies, the advent of the Cold War caused a

---

[94] Act of Oct. 6, 1917, ch. 95, 40 Stat. 394 (1917) ("[W]henever. . . . the publication of an invention by the granting of a patent might, in the opinion of the Commissioner of Patents, be detrimental to the public safety or defense or might assist the enemy or endanger the successful prosecution of the war he may order that the invention be kept secret and withhold the grant of a patent until the termination of the war.").

[95] Of note is the approval of then acting secretary of the navy, Franklin D. Roosevelt, who would have opportunity to revisit this prohibition. S. REP. NO. 65-119, at 3 (approval of Acting Secretary Roosevelt).

[96] *Id.* at 2 ("[W]hen publication of the invention or design . . . might be detrimental to the public safety or the defense of the realm or might otherwise assist the enemy or endanger the successful prosecution of the war, [the Comptroller General of Patents] may delay the acceptance of the complete specification." (citing British Order in Council of October 14, 1915 *in* Patent and Trade-Mark Review, Vol. XIV, 37); *see also id.* (noting a French provision of law empowering the Minister of Commerce to temporarily block patents that would endanger defense).

[97] Indeed, the very text assumed suppression would lift at "the termination of the war." Act of Oct. 6, 1917, 40 Stat. at 394.

[98] Act of July 1, 1940, ch. 501, 54 Stat. 710 (1940).

[99] *Id.*; *see also* Sabing H. Lee, *Protecting the Private Inventor Under the Peacetime Provisions of the Invention Secrecy Act*, 12 BERKELEY TECH. L.J. 345, 349–50 (1997).

[100] Act of June 16, 1942, ch. 415, 56 Stat. 370 (1942); *see also* Lee, *supra* note 99, at 350.

[101] Act of July 2, 1940, ch. 508, 54 Stat. 712–14 (1940). President Roosevelt soon thereafter prohibited the export of petroleum, lead, iron, and steel to Japan. *See Proclamation No. 2417, Signed by President Roosevelt, July 26, 1940*, U.S. DEP'T OF STATE, 3 Bull. 49 (July 27, 1940) *reprinted in* FOREIGN RELATIONS OF THE UNITED STATES, JAPAN, 1931–1941, VOLUME II 216–17 (Joseph V. Fuller ed., U.S. Gov't Printing Office 1943), https://history.state.gov/historicaldocuments/frus1931-41v02/pg_216 [https://perma.cc/9XAQ-N43L].

dramatic shift.[102] The two great inventions of the Second World War, the atomic bomb and the cracking of the German encryption device Enigma,[103] were perceived as vital national resources that could not be disseminated.[104] The Atomic Energy Act (AEA) of 1946[105] forbade patents useful only for nuclear weapons and treated all nuclear information as "born secret,"[106] meaning it was classified from its moment of inception regardless of source.[107] While this categorical approach may have made some sense immediately following a world war,[108] the demands for broader secrecy went much further. In 1951, the Invention Secrecy Act (ISA) inaugurated the possibility of never-ending IP suppression during peacetime; it "established a

---

[102] Alexandra H. Katich, Note, *Innovation Worth Sharing: Seeking Balance Between Innovation Policy and National Security*, 23 CARDOZO J. INT'L & COMP. L. 413, 418 (2015).

[103] The cracking of German naval codes was a necessary step in winning the Battle of the Atlantic, as evinced by enormous Allied losses during a period in which Atlantic U-boats adopted Triton and the information stream went dark. *See* Symposium, *Ultra and the Battle of the Atlantic*, NAT'L SEC. AGENCY DOC ID 3726627 at 6–7, 11 (Oct. 28, 1977), https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/Ultra.pdf [https://perma.cc/H3RC-Q423]; David DiSalvo, *How Alan Turing Helped Win WWII and Was Thanked with Criminal Prosecution for Being Gay*, FORBES (May 27, 2012, 3:06 AM), https://www.forbes.com/sites/daviddisalvo/2012/05/27/how-alan-turing-helped-win-wwii-and-was-thanked-with-criminal-prosecution-for-being-gay/#6a0975dd5cc3 [https://perma.cc/2U5L-38MZ].

[104] NAT'L SEC. AGENCY & CENT. INTELLIGENCE AGENCY, VENONA: SOVIET ESPIONAGE AND THE AMERICAN RESPONSE 1939–1957 (1996), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/venona-soviet-espionage-and-the-american-response-1939-1957/preface.htm [https://perma.cc/9CU2-4WMJ] (noting codebreaking efforts directed against the Soviet Union immediately after the war); Oscar M. Ruebhausen & Robert B. von Mehren, *The Atomic Energy Act and the Private Production of Atomic Power*, 66 HARV. L. REV. 1450, 1450 (1953).

[105] Atomic Energy Act of 1946, ch. 724, 60 Stat. 755, 768 (1946).

[106] *See generally* Howard Morland, *Born Secret*, 26 CARDOZO L. REV. 1401 (2005) (defining and lambasting the term).

[107] Atomic Energy Act of 1954, Pub. L. No. 703, 68 Stat. 919, 924 (1954) (Treating as restricted "[a]ll data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy.").

[108] It should be noted that this direction was not inevitable, however. Famously, Graves thought that patent would be the ideal way to prevent the spread of nuclear secrets. *See* Alex Wellerstein, *Patenting the Bomb*: *Nuclear Weapons, Intellectual Property, and Technological Control*, 99 ISIS J. OF THE HIST. OF SCI. SOC'Y 57, 58-59 (2008), http://alexwellerstein.com/publications/wellerstein_patentingthebomb(isis).pdf [https://perma.cc/8PPW-V2Y9] ("Captain Lavender explained that his office, on behalf of the U.S. government, had filed patent applications for all aspects of bomb manufacture in secret under the authority of the Commissioner of Patents because it had been feared that private inventors might file speculative patent applications and believed that the 'first-to-file' status of the U.S. government would help in potential interference lawsuits. Rather than answering the question of why the Manhattan Project had turned to the patent system, Lavender's answer begged it. The senators were skeptical. 'I didn't dream, frankly, up until this point,' McMahon said, addressing a fellow senator and committee member, 'that there was a patent application down there showing how the bomb was put together. Did you?' 'No,' the other senator replied. 'Personally, I regret it.'").

prior restraint on government employees and . . . private inventors."[109] The ISA limited secrecy orders to a year, but gave the Commissioner the opportunity for constant renewals.[110]

The statutes have not been markedly revised since this time,[111] but there have been attempts to broaden the doctrine. In 2012, the Federal Register solicited comments in light of a congressional request to the U.S. Patent and Trademark Office (USPTO) to determine "whether the currently performed screening of patent applications for national security concerns should be extended to protect *economically significant* patents from discovery by foreign entities."[112] Nothing came of this solicitation. The desire to expand[113] and merge invention secrecy, a limited wartime doctrine that has crossed into perpetual application, and economically-motivated copyright and trade secret doctrines, however, is quite obvious.[114]

The sensitivity of nuclear information has facilitated judicially enforced prior restraint of speech. While prior restraint is exceedingly rare, it appears to have been exercised in both the context of the AEA and the DMCA.[115] In 1950, the Atomic Energy Commission (AEC) ordered *Scientific American* magazine to destroy printed copies and stop publication of an article by Hans Bethe[116] concerning thermonuclear fusion.[117]

---

[109] Laura K. Donohue, *Terrorist Speech and the Future of Free Expression*, 27 CARDOZO L. REV. 233, 275 (2005).

[110] *See* 35 U.S.C. § 181 (2012) ("An invention shall not be ordered kept secret and the publication of the application or the grant of a patent withheld for a period of more than one year. The Commissioner of Patents shall renew the order at the end thereof, or at the end of any renewal period, for additional periods of one year . . . [if the] national interest continues so to require.").

[111] The Atomic Energy Act of 1954 softened restrictions on information related to nuclear power as part of President Eisenhower's Atoms for Peace initiative. RICHARD G. HEWLETT & JACK M. HOLL, ATOMS FOR PEACE AND WAR 1953–1961: EISENHOWER AND THE ATOMIC ENERGY COMMISSION 216 (University of California Press, 1989) (discussing the Atoms for Peace initiative).

[112] Katich, *supra* note 102, at 421.

[113] Oddly, the ISA also become something of a right-wing meme when it was implied that the Obama administration was using the doctrine to prevent the spread of 3D-printed firearms. *See* Danton Bryans, Comment, *Unlocked and Loaded: Government Censorship of 3D-Printed Firearms and a Proposal for More Reasonable Regulation of 3D-Printed Goods*, 90 IND. L.J. 901, 917 (2015) (noting that "some advocate for the use of the Invention Secrecy Act of 1951 (ISA) to control influxes of new technology").

[114] *See* Notice of Request for Comments on the Feasibility of Placing Economically Significant Patents Under a Secrecy Order and the Need to Review Criteria Used in Determining Secrecy Orders Related to National Security, 77 Fed. Reg. 23,662 (Apr. 20, 2012).

[115] *See supra* Section II.A; *see also infra* Section III.A.

[116] *Manhattan Project Spotlight: Hans and Rose Bethe*, ATOMIC HERITAGE FOUND. (Aug. 14, 2014), https://www.atomicheritage.org/article/manhattan-project-spotlight-hans-and-rose-bethe [https://perma.cc/9VFB-BA7N].

Although scientists who read advance copies of the article agreed it contained nothing that had not already been published, the AEC insisted on heavily editing the article.[118] The publisher noted that this prior restraint of "the nation's atomic scientists" indicated that the government was "suppressing information which the American people need in order to form intelligent judgments" on American nuclear policy.[119] Bethe did not wish to press the issue, however, and the matter was never litigated.[120]

Almost thirty years later, in *United States v. Progressive, Inc.*,[121] the government sought an injunction to stop Progressive from publishing an article by Howard Morland titled, "The H-Bomb Secret: How We Got It, Why We're Telling It," which included drawings of a nuclear weapon.[122] Morland, a freelance author with no background in nuclear science, had in large part taken the information for the article from an encyclopedia entry.[123] In granting the injunction under the AEA, the court opined that "[w]hat is involved here is information dealing with the most destructive weapon in the history of mankind, information of sufficient destructive potential to nullify the right to free speech and to endanger the right to life itself."[124] The decision was widely condemned, with the *In These Times* magazine writing, "The Government's attempt to prohibit publication . . . has less to do with anxiety over nuclear proliferation than over the proliferation of legitimate information about the nuclear weapons industry among the American people."[125] The government later dropped the case as moot,[126] thus avoiding Supreme Court review.

---

[117] Wendy Swanberg, The Forgotten Censorship of Scientific American in 1950, Association for Education in Journalism and Mass Communication (Aug. 6, 2008) (unpublished conference paper presented at the Annual Conference of the Association for Education in Journalism and Mass Communication), http://citation.allacademic.com/meta/p_mla_apa_research_citation/2/7/1/6/3/pages271636/p271636-1.php [https://perma.cc/49DZ-L8PL].

[118] *Id.*

[119] HERBERT N. FOERSTAL, TOXIC MIX? A HANDBOOK OF SCIENCE AND POLITICS 13 (2010).

[120] *Id.* at 12.

[121] United States v. Progressive, Inc., 467 F. Supp. 990, 995 (W.D. Wis. 1979).

[122] The original publication, far from a technical manual, looks like a general interest magazine article. *See The H-bomb Secret: How We Got It-Why We're Telling It*, PROGRESSIVE (Nov. 1979), https://www.scribd.com/doc/80517266/The-Progressive-The-H-Bomb-Secret-How-We-Got-It-Why-We-re-Telling-It [https://perma.cc/H86J-8NAL].

[123] FOERSTAL, *supra* note 119, at 13.

[124] *Progressive*, 467 F. Supp. at 995.

[125] FOERSTAL, *supra* note 119 at 14. The recent partial meltdown of the nuclear reactor at Three Mile Island played heavily into coverage of government secret keeping. *See, e.g.*, Douglas E. Kisteeland, *A.C.L.U. Will Represent Editors in Dispute over Article on Bomb*, N. Y. TIMES (Apr. 6, 1979),

B. Export Controls and the Anti-Encryption Movement

While invention secrecy serves as an ideological foundation for the suppression of potentially dangerous IP, the mechanism with the longest global reach is export control. Modern export control springs from the same well as invention secrecy, with wartime embargos of vital material evolving into broad authority to restrict transmission of technical data. The Export Control Act of 1949[127] crafted broad authority for the executive to restrict export licensing of technical data. The Export Administration Act of 1969[128] established the role of the Department of Commerce to administer the Export Administration Regulations for dual use technologies, while the State Department regulated munitions, both of which make up the Commerce Control List.

As noted above, cryptography technology was of paramount concern resulting in cryptography techniques and later, software, being classified as munitions.[129] In barring the dissemination of cryptography, the government retarded development of strong crypto both abroad and at home.[130] While cryptography has never been banned for American citizens, export controls historically barred the dissemination of any key

---

http://www.nytimes.com/1979/04/06/archives/aclu-will-represent-editors-in-dispute-over-article-on-bomb-appeal.html [https://perma.cc/4S38-HKC7] (noting ACLU's statement: "This case is another illustration, like the Pentagon papers case and like the recent Three Mile Island crisis, of the sound First Amendment principle that you cannot trust the Government to decide what the public needs to know.").

126 Free speech supporter and amateur researcher Charles Hansen had sent letters to national newspapers repeating the basic information provided in the article. Upon the publication of one of these letters in the Madison Press Connection, the government concluded that the secret information had been released and dropped the action. *See* Charles R. Babcock & Thomas O'Toole, *H-Bomb Scientists Suspected of Leaks*, WASH. POST (Sept. 20, 1979), https://www.washingtonpost.com/archive/politics/1979/09/20/h-bomb-scientists-suspected-of-leaks/7e9af3be-7ac2-4a31-aeb6-006fea554c84/?utm_term=.a840564e4c22 [https://perma.cc/DL66-B3MS].

127 Act of July 2, 1940, ch. 508, § 6, 54 Stat. 712, 714 (1940) (codified as amended 50 U.S.C. app. §§ 2021–32 (1952)).

128 Export Administration Act of 1969, Pub. L. No. 91-184, 83 Stat. 841 (1969).

129 In effect, encoding triggers were placed in the same category as nuclear triggers. *See* Dan Froomkin, *Deciphering Encryption*, WASH. POST (May 8, 1998), http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm [https://perma.cc/D2T3-R7QC].

130 *See* Bernstein v. U.S. Dep't. of Justice, 176 F.3d 1132, 1146 (9th Cir.) ("Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy.") (internal citations omitted) *en banc reh'g granted & opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

over 40 bits.[131] "[U]nder the International Traffic in Arms Regulations (ITAR), [the data encryption standard] had been treated as something so dangerous that it could only be exported with a license."[132] The National Research Council undercut this approach in 1996 when it released its CRISIS (Cryptography's Role in Securing the Information Society) report.[133] President Clinton issued Executive Order 13206: Administration of Export Controls on Encryption Products, but encryption controls would not be significantly relaxed until 2000.[134]

Of particular interest was the use of export controls to prevent the publication of papers and source code for encryption systems. In 1995, Daniel Bernstein, then a PhD mathematics candidate, sought to publish an encryption system, the source code for that system, and a paper describing the algorithm at the core of the system he created.[135] At the time, export controls would have required Bernstein to register as an arms dealer and submit his paper to the government for prior review. Bernstein challenged these restrictions on First Amendment grounds in federal court.[136] In 1999, four years after he sought to publish, the United States Court of Appeals for the Ninth Circuit affirmed that the code was in fact speech and the export regulations were thus unconstitutional.[137]

---

[131] A. Michael Froomkin, *A Dispatch from the Crypto Wars*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 345, 357–58 (2006) (reviewing MATT CURTIN, BRUTE FORCE: CRACKING THE DATA ENCRYPTION STANDARD (2005)).

[132] *Id.* at 358.

[133] *See generally* NAT'L RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (1996), https://www.nap.edu/read/5131/chapter/1 [https://perma.cc/KNB7-M2R4] (finding that the advantages of an encryption-based information society far outweigh negatives associated with the spread of encryption).

[134] *See* MICHAEL SCHWARTZBECK, THE EVOLUTION OF US GOVERNMENT RESTRICTIONS ON USING AND EXPORTING ENCRYPTION TECHNOLOGIES (Released by CIA Sept. 10, 2014, original date of publication unknown), https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf [https://perma.cc/WU9R-K4T7]; *New Encryption Regulations Still "Overly Complex"*, BIRMINGHAM BUS. J. (Jan. 24, 2000, 12:00 AM CST), https://www.bizjournals.com/birmingham/stories/2000/01/24/story7.html [https://perma.cc/6ALX-JZJ2].

[135] Alison Dame-Boyle, *Remembering the Case that Established Code as Speech*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 16, 2015), https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech [https://perma.cc/W9EN-YVX6].

[136] *See* Bernstein v. U.S. Dep't. of Justice, 176 F.3d 1132, 1132–34 (9th Cir.), *en banc reh'g granted & opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

[137] *Id.* The strange procedural history of Bernstein is worth noting as the decision is not precedential. The government petitioned for and was granted rehearing en banc, resulting in the withdrawal of the panel opinion. However, the en banc rehearing never occurred as the government changed the regulations under judicial review. In January 2000, the government amended export controls to allow for the exemption of publicly available source code. *See* 15 C.F.R. § 740.13(e) (2000). Bernstein argued that this still violated his First Amendment rights and amended his complaint. However, the government successfully argued that as Bernstein had not been

While cryptography export controls have been relaxed significantly since 2000, the War on Terror has occasioned government distaste for publicly available encryption tools and spurred demands for mandated backdoors in encrypted smartphones.[138] The mass shooting in San Bernardino and the resulting debate over encryption on iPhones placed the issue in the public eye.[139] When the FBI demanded that Apple author software unlock the deceased shooter's phone and obtained an order to compel under the All Writs Act, it set up a dramatic legal battle.[140] This confrontation was avoided, however, when the FBI paid more than $1.3 million to a third party for an exploit.[141] Predictably, law enforcement has also called for an end to strong public encryption.[142] Encryption researchers

---

threatened under the new regulations, he lacked standing; *see also* Junger v. Daley, 209 F.3d 481 (6th Cir. 2000) (reversing trial court's finding that encryption source code is not speech protected by the First Amendment and remanding in light of amendments to encryption export regulations); Cindy Cohn, *Nine Epic Failures of Regulating Cryptography*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Sept. 26, 2014), https://www.eff.org/deeplinks/2014/09/nine-epic-failures-regulating-cryptography [https://perma.cc/Q686-SBEZ].

[138] *See* Greg Satell, *The Debate Between the US Government and the Tech Industry About Encryption, Explained*, FORBES (Jan. 9, 2016), https://www.forbes.com/sites/gregsatell/2016/01/09/the-debate-between-the-us-government-and-the-tech-industry-about-encryption-explained/#7e3bb89b7141 [https://perma.cc/4AES-Z59Y].

[139] Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?*, NAT'L PUB. RADIO (Dec. 3, 2016, 1:00 PM ET), http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption [https://perma.cc/4PUC-BQTU].

[140] Amy Davidson Sorkin, *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, NEW YORKER (Feb. 19, 2016), https://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case [https://perma.cc/Q36E-VA35]; *see also Apple Challenges FBI: All Writs Act Order (CA)*, ELECTRONIC FRONTIER FOUND. https://www.eff.org/cases/apple-challenges-fbi-all-writs-act-order [https://perma.cc/2HK2-H8JP].

[141] Julia Edwards, *FBI Paid More than $1.3 Million to Break into San Bernardino iPhone*, REUTERS (Apr. 21, 2016, 2:25 PM), http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB [https://perma.cc/K8NQ-8MSP]. There is a strong argument that the government should release the vulnerability under its Vulnerabilities Equities Process (VEP). Andrew Crocker, *FBI Breaks into iPhone. We Have Some Questions*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Mar. 28, 2016), https://www.eff.org/deeplinks/2016/03/fbi-breaks-iphone-and-we-have-some-questions [https://perma.cc/6AJD-5QF2]. However, in light of the government's stated desire for the creation of a backdoor (that is, a lingering vulnerability), this argument seems fruitless. For more on the VEP, see Andrew Crocker, *EFF Pries More Information on Zero Days from the Government's Grasp*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Jan. 19, 2016), https://www.eff.org/deeplinks/2016/01/eff-pries-more-transparency-zero-days-governments-grasp [https://perma.cc/Y883-7BCB].

[142] Cory Bennett, *Law Enforcement Mobilizes Behind Encryption Bill*, HILL (Apr. 18, 2016, 1:18 PM EDT), http://thehill.com/policy/cybersecurity/276683-law-enforcement-mobilizes-behind-encryption-bill [https://perma.cc/9W4M-UE89]. Similar calls seem to follow any coordinated attack. *See, e.g.*, *The Terrorist in the Data: How to Balance Security with Privacy After the Paris Attacks*, ECONOMIST: BRIEFINGS (Nov. 26, 2015), https://www.economist.com/news/briefing/21679266-how-balance-security-privacy-after-paris-attacks-terrorist-data [https://perma.cc/KY8C-2JDU].

resist such a change, however, arguing that such backdoors will inherently increase complexity and reduce system security.[143]

The interplay of Section 1201 of the DMCA and export controls is intriguing because both purport to serve the national interest by preventing the dissemination of hacking tools. Indeed, in the most recent round of comments on Section 1201, commentators specifically compared these two judicial levers, noting that a relaxed DMCA may be buttressed by more targeted export restrictions.[144] Beyond shared constitutional objections regarding the silencing of speech,[145] these two approaches also trigger common policy questions as to the impact of that enforced silence in the academic context. While export restrictions arguably ceased chilling the publication of encryption papers around 2000, the DMCA began chilling similar research at nearly the same time.

III. DMCA SECTION 1201 STIFLES RESEARCH AND ENCOURAGES VENDOR SECRECY

The DMCA was famously passed to "update copyright law for the digital age."[146] The DMCA introduced many laudable protections for the development of Internet content, but Section 1201 of the act introduced a novel threat to security

---

[143] *See* HAROLD ABELSON ET AL., COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY TECHNICAL REPORT, KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 3 (2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8 [https://perma.cc/42CW-5AP5]; BERKMAN CTR. FOR INTERNET & SOC'Y HARV. UNIV., DON'T PANIC: MAKING PROGRESS IN THE "GOING DARK" DEBATE 2 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/NJ7V-SPNT]; Jonathan Hauenschild, *Encryption is Not Preventing Law Enforcement from Investigating Crime*, AM. LEGIS. EXCH. COUNCIL: PRIVACY & SECURITY BLOG (Feb. 5, 2016), https://www.alec.org/article/encryption-is-not-preventing-law-enforcement-from-investigating-crime/ [https://perma.cc/JAH9-6X5B].

[144] *See* Rebecca Tushnet, *DMCA Hearings, Security Research, Opponents*, TUSHNET.COM (May 26, 2015), https://tushnet.com/2015/05/26/dmca-hearings-security-research-opponents/ [https://perma.cc/54DN-DSHC] (noting that administration considered strengthening export controls as means to prevent information-sharing agreements from strengthening enemies).

[145] Had the court upheld an order forcing Apple to author code to break its own encryption, this would represent yet another constitutional violation in the form of compelled speech. *See* Kim Zetter, *Apple May Use a First Amendment Defense in that FBI Case. And It Just Might Work*, WIRED (Apr. 25, 2016, 7:00 AM), https://www.wired.com/2016/02/apple-may-use-first-amendment-defense-fbi-case-just-might-work/ [https://perma.cc/94L6-Z5NJ].

[146] U.S. COPYRIGHT OFFICE, REPORT ON COPYRIGHT AND DIGITAL DISTANCE EDUCATION 2 (1999); *see also* Hillary A. Henderson, *The Evolution of the Digital Millennium Copyright Act: Changing Interpretations of the DMCA and Future Implications for Digital Copyright Holders*, 42 AIPLA Q.J. 245, 246–47 (noting purpose of act was "to update copyright law for the digital age").

development. Although previous copyright law had regulated *uses* of works in light of the property rights held by the rights holder, Section 1201 sought to restrict user *access* to works. Section 1201 of the DMCA, nominally a law concerned with copyright, created an independent anticircumvention right, with chilling effects squarely in line with previous wartime IP doctrines. Due to the DMCA's focus on stopping copyright infringers from breaching access controls to pirate works,[147] the act has served to stymie security testing and encryption research at the very moment those tasks are most critical. This Section details the anticircumvention provisions of the DMCA, the case law interpreting those provisions, the failure of exemptions to address researcher concerns, and the chilling impact of the provisions.

A. Section 1201: An Independent Anticircumvention Right

Section 1201 has three anticircumvention segments of note. Section 1201(a)(1)(A) states that "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[148] Section 1201(a)(2) prohibits trafficking in tools that enable circumvention of access controls.[149] And Section 1201(b)(1) prohibits trafficking in tools that enable circumvention of

---

[147] While the DMCA Section 1201 shares many features of the national security-focused anti-encryption doctrine, the primary proponent of the section was the motion picture industry. The Motion Picture Association of America had for years pushed the agenda of resting liability on developers and traffickers of circumvention technology, but industry efforts had been fruitless. The push to adopt anticircumvention laws, well documented by Pamela Samuelson, first yielded Article 11 of the WIPO Copyright Treaty, requiring signatories to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures" necessary to protect creative works. Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 414 n.261 (1997).

> The impetus for this provision came largely from the U.S. motion picture industry, which has for many years been keen on the idea of regulating technologies that enable infringement. Although unsuccessful in previous efforts to persuade Congress to pass a broad law to allow them to sue makers of circumvention technologies, the motion picture industry saw in the Clinton administration's National Information Infrastructure (NII) intellectual property initiative a new opportunity for getting the desired legislation.

Id. at 410. Although the obligations of Article 11 are modest, anticircumvention proponents used these requirements to advance and pass the DMCA.

[148] 17 U.S.C. § 1201(a)(1)(A) (2012).

[149] *Id.* § 1201(a)(2). Violation of either of these provisions creates a private right of action for the rightsholder and, should the violation be for a commercial purpose, criminal liability resulting in up to $1,000,000 in fines and ten years of imprisonment. *Id.* §§ 1204(a), 1205.

technological measures that protect the copyright owner's Section 106 rights.[150]

Though the DMCA's anticircumvention provision is commonly thought of in the context of copyright, the provision's scope is far broader. The relationship between Section 1201(a)(2)'s prohibition of circumvention tools that bypass measures "effectively control[ing] access to a work"[151] and Section 1201(b)'s prohibition of circumvention tools that bypass measures "effectively protect[ing] a right of the copyright owner"[152] has caused confusion as to whether Section 1201(a) requires a nexus with infringement. The Federal Circuit viewed Section 1201(a) through the limited lens of conventional copyright infringement, while the Second and Ninth Circuits crafted a new anticircumvention right.[153]

The Federal Circuit, in *Chamberlain Grp., Inc. v. Skylink Tech.'s, Inc.*,[154] attempted to narrow the reach of the anti-trafficking provision, Section 1201(a)(2). The case involved two manufacturers of universal garage door openers.[155] Chamberlain marketed a higher-security rolling code opener that would alter a remote signal to thwart burglars who were detecting and recording valid remote signals.[156] Skylink released a system that was designed to work for both traditional and rolling-code garage door openers.[157] Chamberlain sued, alleging that Skylink's system circumvented the protection mechanism embodied by Chamberlain's rolling code.[158]

The Federal Circuit affirmed the action's dismissal.[159] In essence, the *Chamberlain* court determined that Section

---

[150] *Id.* § 1201(b)(1).

[151] *Id.* § 1201(a)(2).

[152] *Id.* § 1201(b).

[153] *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 950 (9th Cir. 2010); Chamberlain Grp., Inc. v. Skylink Tech.'s, Inc., 381 F.3d 1178, 1183, 1203 (Fed. Cir. 2004); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443–44 (2d Cir. 2001). While the Audio Home Recording Act, 17 U.S.C. § 1002(a)–(c) (2012), has a narrow ban on circumventing devices, it contains no express prohibition on the act of circumvention. Similar acts are generally constrained to prohibited devices, including cable service descramblers (so-called "black boxes") in the Cable Communications Policy Act, 47 U.S.C. § 553(a) (2012) and satellite cable programming descramblers in the Satellite Decryption Provisions of the Communications Act, 47 U.S.C. § 605(e)(3)–(4) (2012). *Accord* Protection of Encrypted Program-Carrying Satellite Signals, North American Free Trade Agreement, Can.-Mex.-U.S., art. 1707, Dec. 17, 1992, 32 I.L.M. 605, 613 (1993).

[154] *Chamberlain Grp., Inc.*, 381 F.3d at 1203.

[155] *Id.* at 1183.

[156] *Id.*

[157] *Id.* at 1184.

[158] *Id.* at 1185.

[159] *Id.* at 1204.

1201(a) created a new cause of action linked to copyright infringement, rather than a standalone (and entirely novel) right of anticircumvention.[160] Accordingly, Chamberlain could not make out a Section 1201(a)(2) claim because

> Chamberlain neither alleged copyright infringement nor explained how the access provided by the [Skylink] transmitter facilitates the infringement of any right that the Copyright Act protects. There can therefore be no reasonable relationship between the access that homeowners gain to Chamberlain's copyrighted software when using Skylink's . . . transmitter and the protections that the Copyright Act grants to Chamberlain.[161]

Two other circuits have held, however, that Section 1201(a)(1)(A) applies to circumvention even when there is no connection to copyright infringement. In *Universal City Studios, Inc. v. Corley*,[162] the Second Circuit upheld an injunction that barred posting code for or links to DeCSS, a computer program that defeated a DVD encryption, Content Scramble System (CSS).[163] Notably, the case appeared to raise fewer antitrust concerns than *Chamberlain* and *Lexmark*. In *Corley*, the court noted that the DMCA was concerned with the preservation of "digital walls" guarding protected material and "does not concern itself with the *use* of those materials after circumvention has occurred."[164]

Similarly, in *MDY Indus., LLC v. Blizzard Entm't, Inc.*,[165] the Ninth Circuit considered the scope of Section 1201(a)(2) in relation to a bot maker.[166] Blizzard is a video

---

[160] *Id.* at 1195 ("Defendants who traffic in devices that circumvent access controls in ways that facilitate infringement may be subject to liability under § 1201(a)(2). Defendants who use such devices may be subject to liability under § 1201(a)(1) whether they infringe or not. Because all defendants who traffic in devices that circumvent rights controls necessarily facilitate infringement, they may be subject to liability under § 1201(b). Defendants who use such devices may be subject to liability for copyright infringement. And finally, defendants whose circumvention devices do not facilitate infringement are not subject to § 1201 liability.").

[161] *Id.* at 1204 (emphasis omitted); *accord* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 552 (6th Cir. 2004) (Merritt, J., concurring) (noting that a broader reading of 1201(a) in the context of printer ink cartridges "would ignore the . . . main point of the DMCA—to prohibit the pirating of copyright-protected works such as movies, music, and computer programs" and would present antitrust concerns).

[162] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443–44 (2d Cir. 2001).

[163] DeCSS was authored by Jon Johansen to allow DVD playback on computers running Linux, which did not support licensed DVD players at that time. *Id.* at 437.

[164] *Id.* at 443.

[165] 629 F.3d 928, 950 (9th Cir. 2010), *as amended on denial of reh'g*, (Feb. 17, 2011).

[166] In this context, a bot means an automated video game character that would normally be controlled by a player. *See* Note, *Spare the Mod: In Support of Total-*

game company with a popular massively-multiplayer online role-playing game called World of Warcraft.[167] MDY Industries marketed a piece of software, "Gilder," that automatically played the game without user input, allowing game players' characters to accrue experience even if game players were not actively playing.[168] Users complained about this cheat mechanism, claiming it disrupted the game playing experience for the wider community.[169] In response, Blizzard banned the use of the bot and designed Warden, a program to assess whether a user connecting to a game server was using the bot.[170] In turn, MDY modified their bot to run only after Warden had completed its assessment of the player's random access memory (RAM).[171] MDY sought a declaration that Glider did not violate Blizzard's copyright rights.[172] Blizzard brought suit alleging numerous copyright violations, including a claim that Glider circumvented the Warden software in violation of Section 1201(a).[173]

A central issue on appeal concerned the nexus between the anticircumvention right and infringement. That is, even if Warden were considered an effective access control, the defeat of Warden merely allowed game players to play a game—an act that did not infringe on a right of Blizzard under the Copyright Act. The court held that the plain text of Section 1201(a) "creates a new anticircumvention right distinct from copyright infringement" and thus reaches anticircumvention unrelated to infringing uses.[174]

In sum, the case law does not provide a sufficient judicial barrier on the application of Section 1201 outside the context of clear copyright infringement. Due to the expansive reach of Section 1201, additional importance falls on specific exemptions. Unfortunately, these too are insufficient.

Conversion Modified Video Games, 125 HARV. L. REV. 789, 792 (2012) (examining bots in online game communities).

[167] *MDY*, 629 F.3d at 935.

[168] *Id.* at 935–36.

[169] *Id.* at 936. Complaints about bots in World of Warcraft are common. *See, e.g.*, ToloDK, *WoW PvP—Too many Bots in Battlegrounds!*, YOUTUBE (Nov 26, 2012), https://www.youtube.com/watch?v=HgWWSJwzEIU [https://perma.cc/67K3-DT5V].

[170] *MDY*, 629 F.3d at 936.

[171] *Id.*

[172] *Id.* at 936–37.

[173] *Id.* at 937.

[174] *Id.* at 948.

B. Statutory Research Exemptions Are Ineffective Due to Narrowness and Lack of Certainty

The authors of the DMCA attempted to address the inevitable deleterious effects that the anticircumvention right would have on scholarly research and data security in two ways. First, through permanent statutory exemptions and, second, through temporary three-year exemptions adopted by the Copyright Office. Neither of the proposed approaches is satisfactory, however, due to either the vague nature of the exemptions or due to their arbitrary impermanence.

The DMCA contains several exemptions so as not to chill necessary research: Section 1201(f) provides an exemption for reverse engineering,[175] Section 1201(g) provides an exemption for encryption research,[176] and Section 1201(j) provides an exemption for security testing.[177] These

---

[175] Specifically, the exemption provides that:

> [A] person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

17 U.S.C. § 1201(f)(1) (2012).

[176] Specifically, the exemption provides that:

> [I]t is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—
>
> (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
>
> (B) such act is necessary to conduct such encryption research;
>
> (C) the person made a good faith effort to obtain authorization before the circumvention; and
>
> (D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

Id. § 1201(g)(2).

[177] Specifically, the exemption provides that:

> [I]t is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

Id. § 1201(j)(2).

exemptions, however, rely on multifactor tests[178] that provide little certainty ex ante that researchers may be free from frivolous suit. Moreover, Section 1201(j) provides little protection in light of the fact that a researcher who exceeds authorization—as may occur with a security researcher because of restrictive licensing terms—would face liability under the Computer Fraud and Abuse Act (CFAA).[179]

Section 1201(g) also required the Copyright Office to generate a report about the impact of Section 1201 on encryption research one year after the DMCA's passage. This report had a narrow window that captured very little of a long-gestating academic research cycle, and was naturally based on speculative comments on the potential effects of the DMCA on

---

[178] Encryption research factors:

> Factors in determining exemption—In 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 encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;
>
> (B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and
>
> (C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

Id. § 1201(g)(3).
Security testing factors:

> Factors in determining exemption—In 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.

Id. § 1201(j)(3).

[179] *See* Erik Stallman, T*he Current DMCA Exemption Process Is a Computer Security Vulnerability*, CTR. FOR DEMOCRACY & TECH. (Jan. 21, 2015), https://cdt.org/blog/the-current-dmca-exemption-process-is-a-computer-security-vulnerability/ [https://perma.cc/3T2C-VKM7]; Charles S. Wood, Note, *Cannibal Cop Out: Why Lenity Is a Necessary, Yet Unworkable Solution in Interpreting the Computer Fraud and Abuse Act*, 82 BROOK. L. REV. 1849, 1852–59 (2017) (detailing the history and broadening of the Computer Fraud and Abuse Act).

both encryption development and research.[180] As such, the Copyright Office found that there had been no "current, discernable impact on encryption research," rendering potential recommendations for alterations "premature."[181]

The chilling effects resulting from the DMCA are not some abstract or new concern. Rather, academics and ethical hackers have constantly noted the impediment of Section 1201 on encryption and security research.[182] From the earliest rounds of rulemaking following the passage of the DMCA, researchers have pleaded for broader protections in the face of corporate threats.[183] In 2000, the Copyright Office noted that

> [a] number of commenters urged that a broader encryption research exemption is needed than is contained in section 1201(g). . . . Dissatisfaction was expressed with the restrictiveness of the requirement to attempt to secure the copyright owner's permission before circumventing. Most of the references to statutory deficiencies regarding encryption research, however, merely state that the provisions are too narrow.[184]

The Copyright Office released another assessment of Section 1201 in June 2017.[185] The results show some incremental progress in accepting the urgency of security testing, but also demonstrate that the current statutory exemptions are inadequate. The report had four key findings with regard to Section 1201(j):[186]

> a) The "authorization" requirement for Section 1201(j) is too inflexible. Section 1201(j) currently "requires researchers to obtain authorization of the owner or operator of [the relevant] computer, computer system, or computer network." This requirement has been criticized as barring meaningful independent security testing if the owner is unreachable or simply unwilling to grant authorization.

---

[180] *See generally* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

[181] *Joint Study of Section 1201(g) of The Digital Millennium Copyright Act*, U.S. COPYRIGHT OFFICE (May 2000), https://www.copyright.gov/reports/studies/dmca_report.html [https://perma.cc/3YFL-SZ2Q].

[182] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,571 (Oct. 27, 2000) (codified at 37 C.F.R. pt. 201); *see infra* Section III.D.

[183] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,571; *see infra* Section III.D.

[184] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,571.

[185] U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS (June 2017), https://www.copyright.gov/policy/1201/section-1201-full-report.pdf [https://perma.cc/9P8Z-UUQ7].

[186] *Id.* at 71–82.

> The report recommends this requirement be removed or made more flexible by taking owner availability into account.[187]
>
> b) The multifactor test for Section 1201(j) is too narrow.[188] The exemption requires that the results of the research be used "solely" to promote the security of the computer owner. This requirement is overly narrow because research could be undertaken to benefit the general public. The report recommended this provision be clarified.[189]
>
> c) This exemption does not preclude compliance with other laws. Though the exemption applies only in cases where no laws are broken, including the CFAA, the report did not find this to be a burdensome requirement. The report noted the issue could be revisited at a later date.[190]
>
> d) Applications for exemption renewal will be streamlined. While exemptions granted through review are temporary and carry no presumption of renewal, proponents of renewal may submit a shorter application.[191]

The report is noteworthy for recognizing that independent security researchers are a key component of increased security. But the report achieves little, and merely tinkers on the margins of unclear statutory exemptions and a broken exemption process.[192]

C. The Triennial Review Process Is Deeply Flawed

The exemption process of the DMCA is a famously broken approach that aims to mildly weaken Section 1201's chilling effect on lawful activities. Once every three years, the public may petition the Copyright Office for an exemption of Section 1201(a)(1)'s restrictions as they relate to a specific class of copyrighted works.[193] For example, past petitions have asked

---

[187] *Id.* at 76–77.

[188] *Id.* at 77–79.

[189] *Id.* at 77.

[190] *Id.* at 79–80.

[191] *Id.* at 140–47.

[192] Mitch Stoltz, *Copyright Office Proposes Modest Fixes to DMCA 1201, Leaves Fundamental Flaws Untouched*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (June 28, 2017), https://www.eff.org/deeplinks/2017/06/copyright-office-proposes-modest-fixes-dmca-1201-leaves-fundamental-flaws [https://perma.cc/VL8D-UACK].

[193] The relevant statute provides:

> In conducting such rulemaking, the Librarian shall examine—
>
> (i) the availability for use of copyrighted works;
>
> (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

for the right to circumvent restrictions on a smartphone so that it could join a wider variety of telecommunication networks (so-called "jailbreaking").[194] The Copyright Office makes recommendations to the Library of Congress, which makes the final determination of whether there can be an exemption on the basis of whether "noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected" by the prohibition.[195]

The Copyright Office engages in a balancing test, which effectively considers the rights of the copyright holder and users of that work. The test illuminates the narrow focus of the exemption process. National security concerns are not formally part of the process, although it does appear that the office occasionally mentions cyberthreats when prompted by exemption opponents.[196] In any event, the Copyright Office lacks the expertise to weigh in on such matters, but even so, the national security implications[197] of proposed exemptions have thrust the Copyright Office into roles for which it is severely underqualified.

This paradox is highlighted in inter-agency communications urging the Copyright Office to restrict itself to

---

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

17 U.S.C. § 1201(a)(1)(C) (2012).

194 Timothy B. Lee, *Jailbreaking Now Legal Under DMCA for Smartphones, but Not Tablets*, ARSTECHNICA (Oct. 25, 2012, 6:45 PM), https://arstechnica.com/tech-policy/2012/10/jailbreaking-now-legal-under-dmca-for-smartphones-but-not-tablets/ [https://perma.cc/6GXV-LKT6] (noting that arbitrary rulings illustrate fundamental brokenness of the DMCA).

195 17 U.S.C. § 1201(a)(1)(D) (2012).

196 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,956 (Oct. 28, 2015) (codified at 37 C.F.R. pt. 201) ("[T]he Register concluded that the record did not support the open-ended exemption urged by Class 25 proponents, encompassing all computer programs on all systems and devices, including highly sensitive systems such as nuclear power plants and air traffic control systems, and that the exemption should be limited to the consumer-oriented uses that were the focus of proponents' submissions.").

197 *See* Comments of Comput. & Commc'ns Indus. Ass'n & Open Source and Indus. Alliance, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, No. RM 2005-11 at 5, https://www.copyright.gov/1201/2006/comments/schruers_ccia.pdf [https://perma.cc/8VNH-EHLE] (requesting exemption for works or compilations distributed in formats protected by access control measures which threaten critical infrastructure and potentially endanger lives).

copyright matters. In a letter to the Copyright Office, the National Telecommunications and Information Administration

> urge[d] the Copyright Office against interpreting the statute [section 1201(a)(1)(C)(v) allowing the Librarian to consider "other factors as the Librarian considers appropriate"] in a way that would require it to develop expertise in every area of policy that participants may cite on the record. Although Congress clearly included this factor to enable consideration of issues not otherwise enumerated, the deliberative process should not deviate too far afield from copyright policy concerns.[198]

The chief problem, as the Register of Copyrights noted in 2010, is that "[n]o other agency has delegated authority to temporarily limit the application of the prohibition on circumvention."[199] The Copyright Office is fundamentally unequipped to consider national security concerns, yet it is the final say on exemptions that weigh directly on those concerns.[200]

National security concerns were certainly not the main driver of the adoption of the DMCA, but they have played a role in perversely thwarting or narrowing exceptions to the DMCA. The dual role of the DMCA, as both national security safeguard and copyright protector, stems in part from our dual conception of hackers as both cyber-terrorists and content thieves alike. While the Copyright Office is charged with weighing the likely benefits and harms to the rights holder and to non-infringing users, opponents of exemption often frame arguments in terms of security.

For example, in successfully seeking to narrow an exemption relating solely to consumer products, the Intellectual Property Owners Association raised the specter of catastrophic public risk due to nuclear meltdown or train derailment, noting that the exemption would reach

> car components, supervisory control and data acquisition systems, and other critical infrastructure, such as the computer code that controls nuclear power plants, smartgrids, and industrial control systems, internet-enabled consumer goods in the home, and transit

---

[198] Opinion Letter on Sixth Triennial Section 1201 Rulemaking from U.S. Dep't of Commerce Nat'l Telecomms. & Info. Admin., Recommendations of the Nat'l Telecomm. & Info. Admin. to the Register of Copyrights at 4 (Sept. 18, 2015), https://copyright.gov/1201/2015/2015_NTIA_Letter.pdf [https://perma.cc/NU64-3CRQ].

[199] *Id.*

[200] *Id.* at 4–5.

> systems. In view of the vast array of products that could be accessed through the exemption, the public risk is impossible to quantify.[201]

Similarly, opposing an exemption for exploration of car software, General Motors (GM) repeatedly mentioned cybersecurity:

> GM's TPMs are strategically designed and implemented to protect vehicle occupant safety (GM's highest priority) and to maintain mandatory emission protections, as well as to thwart illegal activities such as cybersecurity attacks, theft, odometer fraud, modifications to air bag systems, and warranty fraud. . . . GM incorporates TPMs into its vehicle system designs to avoid leaving connected vehicles vulnerable to cyberattack. Allowing consumers of vehicle-based telematics services to switch wireless network providers, or access the underlying software that currently connects in-vehicle telematics systems to a specific wireless provider, would remove this protection without offering GM a comparable alternative for ensuring compliance with important regulatory requirements and protecting vehicle safety, privacy and security.[202]

The exemption process provides a temporary, narrow exception that has no guarantee of renewal. The Librarian of Congress has failed to revive many exemptions in the past, undermining any certainty or freedom from liability intended by the exemption. Prominent failures to renew have involved Internet blocklists and the right to test certain Digital Rights Management tools for malicious code.[203] The exemption

---

[201] Intellectual Property Owners Ass'n, Comment Letter on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201—Sixth Triennial DMCA Rulemaking—Proposed Class 25 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2025/Intellectual_Property_Owners_Association_Class25_1201_2014.pdf [https://perma.cc/7ABE-4ZQA].

[202] General Motors, LLC, Comment Letter on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Proposed Class 13, Unlocking-Mobile Connectivity Devices, No. 2014-07 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2013/General_Motors_class13_1201_2014.pdf [https://perma.cc/Z5VH-8S6E]; *see also* Comment Letter from General Motors, LLC, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Proposed Class 25: Security Research, No. 2014-07 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2025/General_Motors_1201_2014.pdf [https://perma.cc/28L2-PT3S]. ("Thus, the Proposed Exemption weakens a vehicle's carefully designed safety and security framework of which TPMs are an integral part and accordingly increases the vehicle safety and security challenges.")

[203] In 2006, an exemption was renewed for

> [s]ound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely

receiving the most attention was the decision to not renew the jailbreaking exception for smartphones,[204] a result so egregious that it resulted in public outcry and forced Congress to step in to restore the practice.[205]

The 2015 rulemaking produced a rule of note. The rule promulgated as 37 CFR § 201.40(b)(7) provided an exemption for

> Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research 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; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following: (A) A device or machine primarily designed for use by individual consumers (including voting machines); (B) A motorized land vehicle; or (C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.[206]

This rule is a mild improvement but contains numerous flaws, not least of which is the fact that this rule had a delayed

---

> for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

Statement of the Librarian of Congress Relating to Section 1201 Rulemaking, U.S. COPYRIGHT OFFICE (Nov. 22, 2006), https://www.copyright.gov/1201/docs/2006_statement.html [https://perma.cc/CY4L-KNXW]. This addressed concerns arising from Sony's BMG copy-protection scandal, in which undisclosed DRM on music CD's installed rootkits on the user's computer that could subsequently be exploited by hackers. *See* Eran Kahana, *Sony's DRM Experience: When Copyright Protection Attacks*, 60 CONSUMER FIN. L.Q. REP. 627 (2006); *Viruses Use Sony Anti-Piracy CDs*, BBC NEWS (Nov. 11, 2005 11:11 GMT) http://news.bbc.co.uk/2/hi/technology/4427606.stm [https://perma.cc/ZM8X-6S36]. This exemption was not renewed in the following cycle. However, in 2010 a similar exemption was granted for DRM in video games. While not nearly as widespread, Ubisoft's UPlay DRM similarly had an exploit that could have allowed hackers to gain remote access to a user's computer. Alec Meer, *Ubisoft Responds to UPlay Security Drama, Issues Patch*, ROCKPAPERSHOTGUN (July 30, 2012, 5:31 PM), https://www.rockpapershotgun.com/2012/07/30/ubisoft-respond-to-uplay-security-drama/ [https://perma.cc/489X-A6KN]. This exemption was not renewed in the 2013 rulemaking.

[204] *See, e.g.*, Jeff Benjamin, *Unlocking a Cell Phone in the U.S. to Become "Illegal" This Weekend*, IDOWNLOAD BLOG (Jan. 24, 2013) http://www.idownloadblog.com/2013/01/24/unlocking-iphone-illegal/ [https://perma.cc/W6AM-FMDL] (noting re-criminalization of jailbreaking); Derek Khanna, *The Law Against Unlocking Cellphones Is Anti-Consumer, Anti-Business, and Anti-Common Sense*, ATLANTIC (Feb. 11, 2013), https://www.theatlantic.com/business/archive/2013/02/the-law-against-unlocking-cellphones-is-anti-consumer-anti-business-and-anti-common-sense/272894/ [https://perma.cc/2TME-YLDV] (accusing law restricting jailbreaking as encouraging crony capitalism).

[205] *See* Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113-144, 128 Stat. 1751 (2014).

[206] 37 C.F.R. § 201.40(b)(7) (2017).

implementation (aside from voting machines), leaving researchers only two years before renewal hearings.[207] The question of what constitutes a device "primarily designed for use by individual consumers" is also unresolved. Moreover, the "good faith" restriction limits the reach of the exemption to dedicated research in a controlled environment, which may chill hobbyists and independent researchers. Last, the rule arrives approximately ten years after researchers noted the Section 1201(j) statutory exemption would specifically harm research on voting machine security as it would "exclude testing of individual software per se" and that it would limit testing and dissemination in such a way as to "exclude amateur testers."[208]

D. Resulting Chilling Effects of the Anticircumvention Provisions

While proponents of Section 1201 argue that chilling effects are either idiosyncratic or speculative, government experts' and security researchers' testimony tells a very different story.[209] Indeed, former White House Cyber Security Chief Richard Clarke noted the need for DMCA reform because of Section 1201's "chilling effect on vulnerability research."[210] The DMCA crippled the nation's ability to improve electoral infrastructure, in particular, the voting machines that tally votes and the databases that store vital voter information. Moreover, these are the exact targets that were exploited in the recent Russian hacking campaign. This Section details the long-standing complaints of researchers—supported by

---

[207] Kit Walsh, *Why Did We Have to Wait a Year to Fix Our Cars?*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Oct. 28, 2016), https://www.eff.org/deeplinks/2016/10/why-did-we-have-wait-year-fix-our-cars [https://perma.cc/95TW-ZHVY].

[208] Doris Estelle Long, *Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?*, 23 J. MARSHALL J. OF COMPUTER & INFO. L. 533, 547 (2005) (citation omitted).

[209] Matthew Green, *Statement on DMCA Lawsuit*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (July 28, 2016), https://blog.cryptographyengineering.com/2016/07/28/statement-on-dmca-lawsuit/ [https://perma.cc/6FD3-GRYJ]; *see also* Petition for Exemption: Applied Cryptography, Security, and Reverse Engineering Research of Dr. Matthew Green, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, No. 2014-07 (2014), https://copyright.gov/1201/2014/petitions/Green_1201_Initial_Submission_2014.pdf [https://perma.cc/XD3Y-MVZQ]; Comment by Steven M. Bellovin, et al., Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201 (2015), https://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_SecurityResearchers_Class25.pdf [https://perma.cc/ZY58-UK9L].

[210] Hiawatha Bray, *Cyber Chief Speaks on Data Network Security*, BOS. GLOBE (Oct. 17, 2002), https://www.cc.gatech.edu/computing/acmnews/msg00300.html [https://perma.cc/AJ8P-UVRP].

evidence culled from case law and documented threat letters—to show that the DMCA chills disclosure of vulnerabilities to vendors and other academics, as well as chilling research generally. The specific impact on voting machine research highlights the need for and potential impact of broader research freedom in critical infrastructure.

1. Chilling Private Disclosure with Vendors

The DMCA harms researchers' abilities to communicate critical vulnerabilities to vendors. For example, security researcher Mike Davis discovered numerous flaws in the electronic locks put out by Cyberlock.[211] Lock technology implicates national security because these systems are used in metro stations, airports, and data centers.[212] Davis finalized his findings on March 30, 2015, and attempted to disclose them to Cyberlock numerous times over a forty-five day period with little success.[213] As Davis prepared to publish his findings,[214] he received a threatening demand letter from Cyberlock counsel, criticizing his findings and warning that the company "wants to ensure there has been no violation of [its intellectual property] rights, including . . . license agreements or other intellectual property laws such as the anticircumvention provision of the Digital Millennium Copyright Act."[215]

---

[211] Kim Zetter, *With Lock Research, Another Battle Brews in the War over Security Holes*, WIRED (May 6, 2015, 11:14 AM), https://www.wired.com/2015/05/lock-research-another-battle-brews-war-security-holes/ [https://perma.cc/8XEM-BAUY].

[212] *Id.*

[213] Davis noted that he followed Responsible Disclosure, attempting to contact the company six times:

> First notification: March 31, 2015—to Bruce Stephenson, Senior Security Engineer in R&D; Second notification: April 1, 2015—to Support@cyberlock.com; Third notification: April 9, 2015—to CyberLock sales; Fourth notification: April 11, 2015—to Tammy (media relations contact)—Email delivery confirmation received. Fifth notification: April 17, 2015—to CyberLock sales and support; Sixth notification: April 19, 2015—to CyberLock support

Mike Davis, *Security Advisory for Cyberlock Cyberkey*, IOACTIVE (Apr. 30, 2015), https://ioactive.com/pdfs/IOActive_Advisory_CyberLock.pdf [https://perma.cc/6828-VCXX].

[214] *Id.*

[215] Tim Cushing, *Another Company Thinks the Best Way to Handle a Security Hole is to Send a Lawyer After the Person Who Discovered It*, TECHDIRT (May 7, 2015, 10:33 AM), https://www.techdirt.com/articles/20150506/11491630903/another-company-thinks-best-way-to-handle-security-hole-is-to-send-lawyer-after-person-who-discovered-it.shtml [https://perma.cc/A532-7ZSJ] (quoting Letter from Jones Day to Mike Davis (Apr. 29, 2015)).

Understandably, firms would prefer to avoid the embarrassment of disclosing flaws in their products.[216] But, as one commentator pointed out, no one should doubt the deleterious effects of "the approach of seeking to maintain the secrecy of security flaws as a corporate strategy" as this has been "widely discredited as ineffective in the computer security literature."[217] This strategy is damaging on multiple fronts. It prevents correction of problems known in the community, creates an antagonistic relationship between vendors and the security researchers assessing the vulnerability of vendors' products, and creates a culture of inexperience that undermines the appreciation of reported vulnerabilities. "[O]ne such reason [for a mass of vulnerabilities in the smart grid] is that 'many power industry vendors have limited experience dealing with the vulnerability disclosure process. So software vulnerability problems often produce disagreements between vendors and researchers as to the severity of vulnerabilities and appropriate mitigation efforts.'"[218] Sadly, the DMCA permits firms to threaten vendors who seek to expose any such vulnerabilities.

2. Chilling Public Disclosure and Presentation of Cryptography and Security Research at Academic Conferences

The DMCA also hampers researchers' abilities to share their findings with their colleagues. In 2000, the Secure Digital Music Initiative (SDMI) invited researchers to attempt to strip digital watermarks used to protect digital music.[219] Edward

---

[216] David Becker, *Testing Microsoft and the DMCA*, CNET (Aug. 16, 2003, 2:10 PM), https://www.cnet.com/news/testing-microsoft-and-the-dmca/ [https://perma.cc/X3P5-M69S] (discussing Microsoft threat); Declan McCullagh, *Security Warning Draws DMCA Threat*, CNET (Aug. 1, 2002, 9:48 AM PDT), https://www.cnet.com/news/security-warning-draws-dmca-threat/ [https://perma.cc/CDB3-7QJH] (H-P threat against researcher).

[217] Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 824 (2013).

[218] *Id.* at 825 (quoting *What the Power Industry Has to Learn About Cyber Vulnerability Disclosure*, IEEE SMART GRID (Jan. 2012), http://smartgrid.ieee.org/newsletter/january-2012/479-what-the-power-industry-has-to-learn-about-cyber-vulnerability-disclosure [https://perma.cc/FC4K-HVCF].

[219] *SDMI Challenge FAQ*, PRINCETON UNIV. (2000), http://sip.cs.princeton.edu/sdmi/faq.html [https://perma.cc/J29U-YZCW] ("In the first round of the challenge, SDMI provided four 'watermark' challenges and two 'non-watermark' challenges, as described below. For each watermark challenge, three audio streams were presented: a reference stream in its original form, the same stream with a watermark, and a challenge stream, watermarked, with no corresponding reference stream. The challenge was to submit to the SDMI 'oracle' (a Web site), a version of the challenge stream with the watermark removed but without degrading the perceived sound

Felten, a computer science professor at Princeton, along with numerous other researchers at Rice and at Xerox met this challenge.[220] But when SDMI learned that Felten and his team intended to share their results at an academic conference, the Initiative sent demand letters warning of liability under the DMCA.[221] Though the Initiative acknowledged that Felten was not seeking to aid infringement, it nonetheless pressed DMCA claims to ensure Felten would not disclose his findings.

> [T]he purpose of releasing your research is not designed to "help anyone impose or steal anything." Furthermore, your participation in the Challenge and your contemplated disclosure appears to be motivated by a desire to engage in scientific research that will ensure that SDMI does not deploy a flawed system. Unfortunately, the disclosure that you are contemplation [sic] could result in significantly broader consequences and could directly lead to the illegal distribution of copyrighted material. Such disclosure . . . would subject your research team to enforcement actions under the DMCA and possibly other federal laws.[222]

Felten brought suit seeking relief so as to publish his future papers free from fear.[223]

In connection with the resulting lawsuit, numerous researchers and academics submitted declarations asserting that they felt their research was being chilled, with one researcher noting he would not publish his results in similar fields for fear of consequences.[224] Niels Ferguson, a cryptographer in Amsterdam, noted that he had discovered numerous security flaws in HDCP (an encryption used by Intel) but had been "chilled from the recording industry's threats to

---

quality of the original stream. The oracle would respond by email, after several hours, with an 'ACCEPT' message (if the watermark was removed without degrading the sound quality too much) or a 'REJECT' message. In the second round of the challenge, SDMI offered additional 'challenge' tracks to participants who succeeded in defeating the original challenges. No oracle was offered. The SDMI requested that participants send the results of their watermark removal tools along with technical details of how the watermarks were removed. Following this, the SDMI would then offer participants the chance to sign a non-disclosure agreement in return for receiving a fraction of the prize money.").

[220] *Id.*; *see also* Peter Wayner, *Researchers Struggle with Problems from Hiding Data*, COMPUTERWORLD (May 7, 2001, 1:00 AM PT), https://www.computerworld.com/article/2592146/security0/researchers-struggle-with-problems-from-hiding-data.html [https://perma.cc/F4DT-P4P7].

[221] Letter from Matthew J. Oppenheim, Sec'y, The SDMI Found., to Edward Felten, Dep't of Comp. Sci., Princeton Univ. (Apr. 9, 2001), http://sip.cs.princeton.edu/sdmi/riaaletter.html [https://perma.cc/62EB-YQJK].

[222] *Id.*

[223] Felten v. Recording Indus. Ass'n of Am., No. CV-01-2669 (D. N.J. dismissed Nov. 30, 2001).

[224] *See Felten, et al., v. RIAA, et al.*, ELECTRONIC FRONTIER FOUND.: LEGAL CASES, https://w2.eff.org/IP/DMCA/Felten_v_RIAA/ [https://perma.cc/YL8G-5T96] (collecting docket items, including dismissal for lack of standing).

Professor Felten's research."[225] Accordingly, he elected not to publish his findings:

> I have been informed by a U.S. lawyer specialising in this area that even publishing my paper here in the Netherlands will open the door to DMCA prosecution and liability. Not publishing this paper will damage my professional reputation, but if I do publish it I would never be able to visit the U.S. again. This would do me even more harm, both professionally and personally.[226]

Alan Cox, a well-known Welsh programmer with an extensive background in Linux research, noted that

> under the DMCA, I have to choose betweem [sic] keeping quiet when a flaw is known or discovered in an encryption system or other rights management tool, which could put my clients at risk—or being unable to visit the United States without fear of arrest. Without that ability to tell the truth the fight against crime is weakened and the possibility that the national security infrastructure of nations is flawed and weak increases.[227]

These concerns were stoked after Dmitry Sklyarov, a Russian researcher, was arrested soon after giving a conference presentation in the United States on e-book security.[228] Similar fears motivated researchers to consider holding major conferences, like the 2002 IEEE Symposium on Security and Privacy, outside of the United States.[229] Other researchers have taken down their own websites, citing the DMCA.[230]

---

[225] Declaration of Neils Ferguson at ¶ 1–2, 6–8, Felten v. Recording Indus. Ass'n of Am., Inc., (D. N.J. dismissed Nov. 30, 2001) (No. CV-01-2669), ELECTRONIC FRONTIER FOUND.: LEGAL CASES https://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_ferguson_decl.html [https://perma.cc/A66N-PSGU].

[226] *Id.* at ¶ 8.

[227] Declaration of Alan Cox at ¶ 13, Felten v. Recording Indus. Ass'n of Am., Inc., (D. N.J. dismissed Nov. 30, 2001) (No. CV-01-2669)), ELECTRONIC FRONTIER FOUND.: LEGAL CASES https://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html [https://perma.cc/LG8H-DMKH].

[228] *See* Julie Hilden, *The First Amendment Issues Raised by the Troubling Prosecution of E-Book Hacker Dmitry Sklyarov*, FINDLAW (Aug. 10, 2001), http://supreme.findlaw.com/legal-commentary/the-first-amendment-issues-raised-by-the-troubling-prosecution-of-e-book-hacker-dmitry-sklyarov.html [https://perma.cc/Z7K6-6E2E]; Robert Lemos, *Russian Crypto Expert Arrested at Def Con*, CNET (Mar. 2, 2002, 12:05 PM EST) https://www.cnet.com/news/russian-crypto-expert-arrested-at-def-con/ [https://perma.cc/7PQG-2E24].

[229] *See* Declaration of Michael Reiter at ¶ 16, Felten v. Recording Indus. Ass'n of Am., Inc., (D. N.J. dismissed Nov. 30, 2001) (No. CV-01-2669), ELECTRONIC FRONTIER FOUND.: LEGAL CASES https://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_reiter_decl.html [https://perma.cc/MMK6-WGLR].

[230] Ryan W. Maple, *Dug Song Censors Website, Cites DMCA*, LINUXSECURITY.COM (Sept. 9, 2001, 9:55 AM), http://web.archive.org/web/20010911142115/http://www.linuxsecurity.com:80/articles/cryptography_article-3624.html [https://perma.cc/834A-QYTE].

Preventing researchers from communicating and building on each other's findings exacerbates the damage of these chilling effects. Disclosure of discovered vulnerabilities is a fundamental component of security innovation, as noted by technologist Bruce Schneier.

> It is a regular practice in the science for a security researcher to learn from other peoples' breaks. In order for the academic disciplines of cryptography and computer security to advance, a researcher who breaks a security system needs to make his result available to the rest of the research community. As in any other academic discipline, this unfettered free exchange of ideas and research results is the means by which the entire field may benefit from one person's research, strengthening all of society's security as a result.[231]

The prevention of public disclosure of vulnerabilities also prevents corrective market action. As Professor Eugene Volokh observed, "Publishing detailed information about a computer program's security vulnerabilities may. . . . persuade apathetic users that there really is a serious problem [and] persuade the media and the public that some software manufacturer isn't doing its job."[232] A company has strong incentives to avoid drawing attention to vulnerabilities, and therefore attempts to bury them entirely or release muted warnings. If this information is kept from the public, deficient vendors may avoid accountability through reduced consumption of a product and/or constituent pressure on governmental actors to intervene. Even members of Congress who follow a dogged, free-market approach, such as Republican Senator Mike Lee, note the importance of disclosure: "I generally trust the market to create the right incentives for retailers to protect data of their customers. But consumers need notification of data breaches for that to work."[233]

While judicially approved prior restraint[234] is exceedingly rare,[235] the DMCA has been used to bar publication

---

[231] Declaration of Bruce Schneier at ¶ 13, Felten v. Recording Indus. Ass'n of Am., Inc., (D. N.J. dismissed Nov. 30, 2001) (No. CV-01-2669), ELECTRONIC FRONTIER FOUND.: LEGAL CASES, https://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_schneier_decl.html [https://perma.cc/4D8Y-VUYE].

[232] Volokh, *supra* note 4, at 1118.

[233] Kristin M. Bergman, *A Target to the Heart of the First Amendment: Government Endorsement of Responsible Disclosure as Unconstitutional*, 13 NW. J. TECH. & INTELL. PROP. 117, 143 (2015) (quoting *Summary: Target Testifies on Massive Data Breach*, WALL ST. J.: CORP. INTELLIGENCE BLOG (Feb. 4, 2014, 10:38 AM), http://blogs.wsj.com/corporate-intelligence/2014/02/04/live-target-testifies-on-massive-data-breach/ [https://perma.cc/355L-K54V].

[234] The extremely odd anticircumvention provision of the DMCA befuddles researchers and First Amendment scholars alike, in part because the provisions

of DeCSS code, a method of decrypting the Content Scramble System on DVD's, by the magazine *2600: The Hacker Quarterly*.[236] The researcher community responded to this suppression of speech by placing the code on t-shirts and ties, rendering the code in haiku, and recording spoken-word monologues.[237] In light of the caustic response to the ruling, and DeCSS's wide dissemination in spite of the restraint, it is unclear if another court would sanction this sort of chilling censorship.

3. Chilling Efficient Research

While the existence of Section 1201 of the DMCA does not necessarily render impossible certain research topics, it may instead introduce obstacles that result in less efficient research. Matthew Green, a professor of computer science and a security researcher at Johns Hopkins University, detailed two ways in which Section 1201 slows research: by diverting resources from scientific to legal questions[238] and by forcing researchers to adopt indirect methods to avoid running afoul of the law.[239]

---

enshrine an absolute secrecy regime antithetical to both disciplines. Here, the DMCA merges with a more troubling strain of intellectual property doctrine centered on invention secrecy.

[235] *See, e.g.*, N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (Pentagon papers case involving six separate concurrences discussing the doctrines narrowness or inapplicability in matters outside of dire national security); Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 716 (1931) (barring prior restraint in libel and noting that restraint only appropriate in exceptional cases on national security and decency grounds); *see also* Megan L. Shaw, *When the Fourth Estate's Well Runs Dry*, 83 BROOK. L. REV. 701, 705–12 (2018) (detailing history of prior restraint cases).

[236] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 434–35, 439 (2d Cir. 2001).

[237] *See* Seth Schoen, *The History of the DeCSS Haiku*, LOYALTY, http://www.loyalty.org/~schoen/haiku.html [https://perma.cc/VY5D-ZEHC]; David S. Touretzky, *Gallery of CSS Descramblers*, CARNEGIE MELON UNIV. COMP. SCI. DEP'T (2000), http://www.cs.cmu.edu/~dst/DeCSS/Gallery/ [https://perma.cc/6JLE-9UA2].

[238] Green, *supra* note 209 ("Nearly every attempt to analyze a software-based system presents a danger of running afoul of the law. As a result, the first step in any research project that involves a commercial system is never science—it's to call a lawyer; to ask my graduate students to sign a legal retainer; and to inform them that even with the best legal advice, they still face the possibility of being sued and losing everything they have. This fear chills critical security research.").

[239] Green notes that

> [i]n a recent project—conducted in Fall 2015—we were forced to avoid reverse-engineering a piece of software when it would have been the fastest and most accurate way to answer a research question. Instead, we decided to treat the system as a black box, recovering its operation only by observing inputs and outputs. This approach often leads to a less perfect understanding of the system, which can greatly diminish the quality of security research. It also substantially increases the time and effort required to finish a project, which reduces the quantity of security research.

4. Chilling Investigation and Improvement of Voting Machines

The DMCA has had a notorious impact on voting machine security research, with an exemption to the DMCA granted only after a decade of complaints. The DMCA provided two methods to retard public discussion regarding voting machine vulnerabilities: it effectively criminalized the fair-use reverse engineering[240] need to discover vulnerabilities and it also provided a means to prevent dissemination of vulnerabilities.[241] The willingness to abuse the DMCA seems to include voting machine manufacturers, with Diebold and Sequoia issuing baseless threats to hide vulnerabilities. Recent research, itself conducted after a long overdue DMCA exemption, revealed critical flaws in the system that have persisted for decades.

a. Diebold

Diebold used a baseless DMCA copyright claim in an effort to pull down internal emails discussing vulnerabilities. Diebold engineers lamented the state of security on their own machines, writing,

> Our smart-card format has absolutely no security, so if someone were to get a copy of this software and a reader, they could stand at the ballot station and quietly burn new voters cards all day. . . . I can see the cover of USA Today in my head. Consider everyone warned.[242]

When Diebold learned that hacked emails concerning known vulnerabilities had been posted to the Internet, the company sent out multiple DMCA pull-down notices to sites hosting the information as well as sites merely linking to it. Though Diebold was ultimately defeated in court by two Swarthmore students,[243] the episode was an early example of voting systems

---

Id.

[240] That is, provided that such reverse engineering would require circumvention.

[241] Online Policy Grp. v. Diebold, Inc., 337 F. Supp. 2d 1195, 1204–05 (N.D. Cal. 2004) (noting that Diebold behavior shows a desire "to use the DMCA's safe harbor provisions—which were designed to protect ISPs, not copyright holders—as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.").

[242] Barney Gimbel, *Rage Against the Machine: Diebold Struggles to Bounce Back from the Controversy Surrounding Its Voting Machines*, FORTUNE (Nov. 3, 2006, 9:45 AM EST), http://archive.fortune.com/magazines/fortune/fortune_archive/2006/11/13/8393084/index.htm [https://perma.cc/98Z7-MDKK]

[243] *Diebold*, 337 F. Supp. 2d at 1197, 1204.

manufacturers attempting to use the DMCA to hide vulnerabilities.

Diebold was subsequently accused of attempting to thwart third-party testing[244] and spreading misinformation about the certification of their machines.[245] As part of a $2.6 million settlement with the State of California, Diebold agreed to make necessary security enhancements.[246] Prominent among these were the requirement to replace hard-coded (that is, static) features with dynamic features.[247] Diebold was required to "[r]eplace hard-coded supervisor passwords with dynamic passwords" and to "[r]eplace hard-coded Data Encryption Standard (DES) security key with [programmable] encryption keys."[248]

b. Sequoia

Felten, the researcher who was threatened by SDMI and criticized by Diebold, later received a demand letter from Sequoia Voting Systems when the e-voting machine company learned that New Jersey election officials planned to send machines to Felten for analysis.[249] The letter noted "Sequoia has . . . retained counsel to stop any infringement of our intellectual properties, including any non-compliant analysis. We will also take appropriate steps to protect against any publication of Sequoia software, its behavior, reports regarding same or any other infringement of our intellectual property."[250]

---

[244] Ed Felten, *Refuting Diebold's Response*, FREEDOM TO TINKER (Sept. 20, 2006), https://freedom-to-tinker.com/2006/09/20/refuting-diebolds-response/ [https://perma.cc/52S8-HHXG].

[245] *Diebold May Face Criminal Charges*, WIRED (Apr. 23. 2004, 8:55 AM), https://www.wired.com/2004/04/diebold-may-face-criminal-charges/ [https://perma.cc/K7TR-3S5J]; Press Release, Cal. Dep't of Justice Office of the Attorney Gen., Attorney General Lockyer Announces $2.6 Million Settlement with Diebold in Electronic Voting Lawsuit (Nov. 10, 2004), https://oag.ca.gov/news/press-releases/attorney-general-lockyer-announces-26-million-settlement-diebold-electronic [https://perma.cc/N29N-HFW2].

[246] [Proposed] Stipulated Final Judgment and Permanent Injunction at 6, 9–20, California v. Diebold Election Sys., Inc., (Cal. Super. Ct. Nov. 10, 2004) (No. RG 03128466), https://oag.ca.gov/system/files/attachments/press_releases/04-130.pdf [https://perma.cc/F8PE-XR6V]. The latter requirement is telling as DES had been hacked in 1999 and replaced in the US government by the Advanced Encryption Standard in 2002. NAT'L INST. OF STANDARDS & TECH., FIPS PUB. 197, ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) (2001).

[247] [Proposed] Stipulated Final Judgment and Permanent Injunction, *supra* note 246, at 17–19.

[248] *Id.* at 17–18.

[249] Ed Felten, *Interesting Email from Sequoia*, FREEDOM TO TINKER (Mar. 17, 2008), https://freedom-to-tinker.com/2008/03/17/interesting-email-sequoia/ [https://perma.cc/87BS-KTZ5].

[250] *Id.*

This letter was widely derided, with commentators noting "[i]t's hard to imagine a stupider legal threat."[251]

c. DEFCON Hacking Competition Reveals Widespread Vulnerabilities

A recent group hacking exercise demonstrated the myriad of vulnerabilities that exist (and persist) in e-voting machines. Matt Blaze, a professor at the University of Pennsylvania, helped set up a voting machine hacking event at DEFCON, an annual hacking convention.[252] The event involved thirty machines representing the major manufacturers including Sequoia AVC Edge, ES&S iVotronic, Diebold TSX, WinVote, and Diebold Expresspoll 4000.[253] It appears to be the first of its kind, as such activity was illegal under the DMCA until an exemption was created in 2015.[254] The event involved several luminaries in the field, including Harri Hursti, one of the first researchers to hack an e-voting machine.[255]

The results of the event were sobering, with roughly thirty machines hacked using known exploits within the first ninety minutes. A WinVote terminal was hacked using a basic Windows XP exploit dating back to 2003. Indeed, a participant noted that the "[h]ardest part of hacking WINVote was buying a USB keyboard. CTR-alt-delete boots voting machine into Windows XP."[256] The encryption key used for the wireless

---

[251] Cory Doctorow, *Sequoia Voting Systems Threatens Felten's Princeton Security Research Team*, BOING BOING (Mar. 17, 2008 8:47 PM), http://boingboing.net/2008/03/17/sequoia-voting-syste.html [https://perma.cc/QV8N-4BEB].

[252] MATT BLAZE ET AL., DEFCON 25 VOTING MACHINE HACKING VILLAGE REPORT ON CYBER VULNERABILITIES IN U.S. ELECTION EQUIPMENT, DATABASES, AND INFRASTRUCTURE 4 (Sept. 2017), https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf [https://perma.cc/VH3K-XPAC].

[253] *#Votingvillage Is a Hit!*, DEFCON COMMS. INC. (July 28, 2017), https://www.defcon.org/html/defcon-25/dc-25-index.html [https://perma.cc/M96Y-WD4H].

[254] *See* Elizabeth Weise, *Hackers Plan to Break into 30 Voting Machines to Put Election Meddling to the Test*, USA TODAY (July 27, 2017, 9:04 PM EST), https://www.usatoday.com/story/tech/2017/07/26/voting-machines-hackers-election-hack/507071001/ [https://perma.cc/2ZWK-46F8].

[255] *See* DAVID WAGNER ET AL., SECURITY ANALYSIS OF THE DIEBOLD ACCUBASIC INTERPRETER 6 (2006), https://www.sos.state.tx.us/elections/forms/security_diebold_accubasic.pdf [https://perma.cc/R4HB-Z2CA] (detailing the Hursti Hack and noting Hursti's role in spurring concerns on e-voting security); Edward-Isaac Dovere, *Top Hacker Conference to Target Voting Machines*, POLITICO (May 23, 2017, 4:34 PM EDT), http://www.politico.com/story/2017/05/23/defcon-hacker-conference-voting-machines-238734 [https://perma.cc/23UA-8XUU].

[256] Sean Gallager (@thepacketrat), TWITTER (July 29, 2017, 1:33 PM), https://twitter.com/thepacketrat/status/891396377208647681 [https://perma.cc/3K8B-LFUR] (showing hack of voter machine to play Rick Astley's "Never Gonna Give You Up," a common meme known as Rick-rolling); DEFCON VotingVillage

connection on the machine was "abcde."[257] Voter information was also insecure, as hackers "found actual voter reg[istration] data from the 2008 election in . . . plain text" stored on machines.[258]

While the mass researcher hack of voter machines was without precedent, their results were not.[259] As seen from occasions where states have requested audits of voting machines, sloppy protections are the norm.[260] In 2015, the Virginia Information Technologies Agency examined WINVote machines following repeated crashes during the 2014 election.[261] VITA's report recommended

> discontinuing use of the Advanced Voting System WINVote devices . . . [due to] weak security controls used by the devices [that] would not be able to prevent a malicious third party from modifying the votes recorded by the WINVote devices. The primary contributor to these findings is a combination of weak security controls used by the devices, namely, the use of encryption protocols that are not secure, weak passwords, and insufficient system hardening.[262]

(@VotingVillageDC), TWITTER (July 29, 2017, 1:33 PM), https://twitter.com/VotingVillageDC/status/891392969881812993 [https://perma.cc/NA4D-GTDU] (same).

[257] Shuguh Works, *Voting Machine Hacking Village DEF CON 25*, YOUTUBE (July 29, 2017), https://www.youtube.com/watch?v=ADyfcz6MUD4 [https://perma.cc/4PJW-9JLQ].

[258] Sean Gallager (@thepacketrat), TWITTER (July 29, 2017, 2:48 PM), https://twitter.com/thepacketrat/status/891369912119197696 [https://perma.cc/F9CP-KC4V]; Kevin Collier, *Personal Info of 650,000 Voters Discovered on Poll Machine Sold on Ebay*, GIZMODO (Aug. 1, 2017, 2:50 PM), http://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462 [https://perma.cc/3SGX-F9GR].

[259] *See* Weise, *supra* note 254; *see also* Sean Michael Kerner, *Hackers Demonstrate Voting Machine Vulnerabilities at DefCon*, EWEEK (July 28, 2017), http://www.eweek.com/security/hackers-demonstrate-voting-machine-vulnerabilities-at-defcon [https://perma.cc/FF7C-5B6H]; Ben Wofford, *How to Hack an Election in 7 Minutes*, POLITICO (Aug. 5, 2016), http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144 [https://perma.cc/9CEL-XFPS]; *Hacking the Machines—Coverage Finally!*, HOLLER BACK-[NOT] VOTING IN AN AMERICAN TOWN (Aug. 12, 2016), http://www.hollerbackfilm.com/blog/2016/8/6/coverage-on-the-hacking-of-the-machines-finally [https://perma.cc/W7PH-NVHE].

[260] Cory Bennett, *States Ditch Electronic Voting Machines*, HILL (Nov. 11, 2014, 9:00 AM EST) http://thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines [https://perma.cc/5JLE-QAYA] (noting successful efforts to demonstrate vulnerabilities in these machines).

[261] *See generally* VIRGINIA INFORMATION TECHNOLOGIES AGENCY, COMMONWEALTH SECURITY & RISK MANAGEMENT, SECURITY ASSESSMENT OF WINVOTE VOTING EQUIPMENT FOR DEP'T OF ELECTIONS (2015), http://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf [http://perma.cc/4D2G-R535]; Kim Zetter, *Virginia Finally Drops America's 'Worst Voting Machines*,' WIRED (Aug. 17, 2015, 7:00 AM), https://www.wired.com/2015/08/virginia-finally-drops-americas-worst-voting-machines/ [http://perma.cc/G46B-N6VF].

[262] VIRGINIA INFORMATION TECHNOLOGIES AGENCY, *supra* note 261.

Among these weaknesses were the aforementioned "abcde" Wi-Fi password, a failure to patch the system for eleven years, and a hardwired administrator password of "admin."[263] Following the publication of the report, Virginia decertified the machine, roughly seven years after security issues connected to the machines' always-on Wi-Fi first surfaced.[264]

IV. PROPOSAL: ELIMINATING THE INDEPENDENT ANTICIRCUMVENTION RIGHT AND ADOPTING A RESPONSIBLE OPEN COMMUNITY MODEL IN CYBERSECURITY

As should now be obvious, cyber-warfare is prevalent and growing. Moreover, the current approach to intellectual property law in light of national security is deficient, thus crippling our cyber-defense. We must increase transparency while enlisting the aid of academics and altruistic researchers to both prevent and detect intrusions.

This Section details the proposed solution. First, Congress should remove Section 1201(a)(2), limit Sections 1201(a)(1) and 1201(b) to underlying acts of infringement, and encourage independent security researchers ("ethical hackers" or "white hats"). Second, Congress should adopt a cyber risk assessment paradigm to combat reflexive secrecy and strengthen existing assets.

A. Removal of DMCA Section 1201(a)(2) and Establishing a Stringent Infringement Nexus Requirement for Anticircumvention

The Copyright Office appears to realize that the restrictions of Section 1201 pose a serious threat to security research.[265] The Office, however, seeks to address this vital weakness through piecemeal exemptions, doled out in triennial cycles.[266] This is unsurprising, as the Office is primarily focused on balancing the interests of rights holders and users, not the security of the nation. Moreover, rights holders may tap into an outdated IP security doctrine of secrecy to argue against broad security exemptions.

---

[263] Jeremy Epstein, *The Worst Voting Machine in America*, SLATE (Apr. 16, 2015, 1:12 PM), http://www.slate.com/articles/technology/future_tense/2015/04/avs_winvote_virginia_voting_machine_s_password_was_admin.html [http://perma.cc/R6ZJ-BPVN].

[264] Zetter, *supra* note 261.

[265] U.S. COPYRIGHT OFFICE, *supra* note 185, at 71–81.

[266] *Id.* at 140–49.

The urgency of the current climate forces a more direct and logical solution. Section 1201(a)(2) must be repealed, and Section 1201(a)(1) must be amended to cover only circumvention directed to unlawful infringement of *established rights* of copyright holders, rather than creating an intent-free, broad, and novel *access right*. This would bring Section 1201 in line with the Federal Circuit's limited reading of Section 1201 from its decision in *Chamberlain*.[267] Moreover, this approach would eliminate the need for the narrow exemptions, as there are numerous other lawful activities that are not captured by the current exemptions.

Section 1201(a)(1) should therefore be amended as follows: "Circumvention of a technological measure shall not be considered a violation of this title unless that circumvention is undertaken to engage in a use that is an infringement of copyright." Section 1201(a)(2) would thus be removed as redundant of 1201(b).

B. Abandoning Security Through Obscurity in the Realm of Cybersecurity

In order to prevent the invention secrecy doctrine from inexorably pulling policy towards a security through obscurity approach, the government should adopt a responsible open community risk-assessment with regards to cybersecurity. To that end, the government should continue to establish open-ended bounties for vulnerabilities into critical infrastructure. More critically, though, the government should establish itself as an intermediary to facilitate responsible disclosure.

U.S. Computer Emergency Readiness Team (US-CERT), which already solicits information regarding phishing and other malware encounters, should similarly solicit vulnerability information and communicate such vulnerabilities to vendors. While this system of disclosure will not be mandatory, it will likely attract interest from security researchers who are frustrated with vendors' antagonism and lack of response.

C. Responsible Defense in Depth-Open Community Principles

A responsible community approach reflects a defense in depth philosophy. Defense in depth is a "holistic approach—one

---

[267] *See supra* notes 154–161 and accompanying text.

that uses specific countermeasures implemented in layers to create an aggregated, risk-based security posture."[268] An open community harnesses the efforts of researchers to create two additional layers of defense: detection of vulnerabilities to prevent intrusions and detection of odd system behaviors to limit the impact of initially successful intrusions.

The wisdom of this approach centers on three principles: (1) independent researchers (i.e., members of the wider security community) are a vital part of security; (2) hiddenness of defenses decreases in utility as the number of attacks increases; and (3) while disclosure may increase risk in the short term, disclosure is necessary for long-term security. These principles are borne out in the real world and point to responsible openness as the optimal approach in the realm of cybersecurity.

1. Independent Security Researchers Aid in Discovering Vulnerabilities and Detecting Intrusions

Market realities already point to the efficiency of enlisting independent security researchers to detect high-severity security weaknesses. Ethical hackers routinely ferret out and responsibly report vulnerability, often for bounties. Numerous companies run bounty programs in which users are rewarded for discovering exploits. For example, Apple will pay up to $250,000 for iPhone exploits.[269] Exploit brokers, like Zerodium, have offered as much as $1.5 million for exploits.[270] While these are the highest sorts of payments, the average bounty paid to ethical hackers is approximately $2,000.[271]

---

[268] U.S. DEP'T OF HOMELAND SEC., INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM, RECOMMENDED PRACTICE: IMPROVING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY WITH DEFENSE-IN-DEPTH STRATEGIES at III (Sept. 2016), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [https://perma.cc/GS3V-NEFJ].

[269] Dan Goodin, *iPhone Exploit Bounty Surges to an Eye-Popping $1.5 Million*, ARS TECHNICA (Sept. 29, 2016, 7:30 PM), https://arstechnica.com/security/2016/09/1-5-million-bounty-for-iphone-exploits-is-sure-to-bolster-supply-of-0days/ [https://perma.cc/MJ2V-3QMX] (noting that bounties "will also ensure that an ample supply of zeroday exploits remain in the wild, despite the non-trivial strides Apple, Google, and other software makers continue to make in security [sic] their products").

[270] *Id.*

[271] Morgan Chalfant, *Dem Pushes 'Ethical Hacking' Resolution*, HILL (July 19, 2017, 5:25 PM EDT), http://thehill.com/policy/cybersecurity/342803-dem-pushes-ethical-hacking-resolution [https://perma.cc/ZV3S-4DGW].

Google maintains a bug leaderboard as a means to generate interest and praise for bug hunters.[272]

In recognition of the economic and national security benefits of this exploit activity, members of Congress have called for the development of programs that "prepare students for careers in cybersecurity by actively promoting ethical hacking skills."[273] Similarly, the Hack DHS Act was introduced to encourage ethical hacking attempts against the Department of Homeland Security.[274] Similar bug bounty programs have been launched for the Pentagon,[275] Air Force,[276] and Army.[277] The Hack the Pentagon program[278] has been praised as revealing "hundreds of vulnerabilities at a fraction of the cost of commercial penetration testing."[279] Relatedly, agencies have called for the recruitment of ethical hackers to serve as cyber special agents.[280]

---

[272] Taylor Hatmaker, *Google's Bug Bounty Program Pays Out $3 Million, Mostly for Android and Chrome Exploits*, TECHCRUNCH (Jan. 31, 2017), https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/ [https://perma.cc/DQE6-RG8V].

[273] Chalfant, *supra* note 271.

[274] H.R. 2774, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/2774/text?r=21 [https://perma.cc/97SH-PRPT]; Maggie Hassan & Rob Portman, *Why We're Encouraging Ethical Hackers to Try and Hack the Department of Homeland Security*, TIME (June 30, 2017), http://time.com/4837557/hackers-homeland-security-cyber-attacks/ [https://perma.cc/GH4L-652N].

[275] *'Hack the Pentagon' Pilot Program Opens for Registration*, DOD NEWS (Mar. 31, 2016), https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration/ [https://perma.cc/5CDJ-KWHM]; #RSAC: *US Government Bug Bounty Programs Here to Stay Under Trump Administration*, INFOSECURITY (Feb. 14, 2017), https://www.infosecurity-magazine.com/news/rsac-us-government-bug-bounty/ [https://perma.cc/B8VM-785X].

[276] Kate Conger, *Air Force Launches Bug Bounty Program*, TECHCRUNCH (Apr. 26, 2017), https://techcrunch.com/2017/04/26/air-force-launches-bug-bounty-program/ [https://perma.cc/MD9H-V67U].

[277] Mark Rockwell, *Why Bug Bounty Programs Are Worth the Risk*, FCW (Mar. 30, 2017), https://fcw.com/articles/2017/03/30/bug-bounties-gsa-dod.aspx [https://perma.cc/QUT2-GUDX].

[278] Meredith Somers, *Lessons Learned from DoD's Bug Bounties Highlight Gaps in Talent, Secrecy*, FED. NEWS RADIO (Mar. 30, 2017, 6:07 PM), https://federalnewsradio.com/cybersecurity/2017/03/lessons-learned-from-dods-bug-bounties-highlight-talent-gap-secrecy-is-not-security/ [https://perma.cc/J2PN-EBVQ].

[279] Rockwell, *supra* note 277. Of course, the government is more likely to attract grey hat hacking, in part because the CFAA does not apply to government security testing. *See* Andrea O'Sullivan, *The Economics of Software-Vulnerability Sales: Can the Feds Encourage 'Pro-Social' Hacking?*, REASON (Aug. 11, 2015), https://reason.com/archives/2015/08/11/economics-of-the-zero-day-sales-market [https://perma.cc/836T-5P68] (noting that while grey hats may be helpful, the ultimate goal of government should be to encourage white hats).

[280] Becky Yerak, *FBI Seeks 'Ethical' Hackers to be 'Cyber Special Agents'*, CHI. TRIB. (Dec. 29, 2014, 2:28 PM), http://www.chicagotribune.com/business/ct-fbi-ethical-hackers-1229-biz-20141229-story.html [https://perma.cc/3CRJ-LL39].

Even in areas without bounties, so-called white hats[281] have used their talents to thwart cyberattacks or expose vulnerabilities.[282] As noted earlier, the WannaCry attack would have been much more virulent but for the actions of an ethical hacker, Marcus Hutchins.[283] Similarly, a group of ethical hackers demonstrated how touch ID systems on both the Apple iPhone[284] and the Samsung Galaxy 5[285] could be easily defeated to gain access to payment software.

---

[281] Hackers are commonly divided into black hats, grey hats, and white hats, following the color scheme of old westerns. *White Hat Hackers and the Future of Cyber Security Monitoring*, MASSIVE MEDIA (Sept. 26, 2016), https://www.massivealliance.com/2016/09/26/white-hat-hackers-future-cyber-security-monitoring/ [https://perma.cc/J62H-3LCQ]. Black hats are malicious hackers who attempt to penetrate and disrupt systems. This may be for financial or political gain or the simple enjoyment of causing chaos, commonly described as "for the lulz." *See, e.g.*, Jack Morse, *Script Kiddies May Be Working to Bring Back WannaCry Just for the Lulz*, MASHABLE (May 19, 2017), http://mashable.com/2017/05/19/wannacry-hackers-ransomware-lulz/#8qfO4pQJcSqj [https://perma.cc/F76V-5543] (Security Researcher Marcus Hutchins noting that a group of hackers attempted to revive WannaCry by knocking out the domain functioning as a kill-switch and ascribing their motivation "it's most likely scriptkiddies [i.e., low skill hackers] doing it for lulz"). Grey-hat hackers attempt to penetrate systems but typically sell the resulting vulnerability. White-hat hackers penetrate systems but do so with either the permission of the target or with the express purpose of exposing the vulnerability. *See* Georg Thomas, *An Ethical Hacker Can Help You Beat a Malicious One*, GCN (May 22, 2017), https://gcn.com/Articles/2017/05/22/ethical-hackers.aspx?Page=1 [https://perma.cc/R6P8-MP66]. It has been noted that "[s]ome white hats are reformed black hats." Paul Gil, *What Are 'Black Hat' and 'White Hat' Hackers?*, LIFEWIRE (Jan. 22, 2018), https://www.lifewire.com/black-hat-hacker-a-white-hat-hacker-4061415 [https://perma.cc/NEU7-EKGN]; *see also* Steve Morgan, *Black-Hat Hackers More Daring and Experienced Than White-Hat Hackers*, CSO (Mar. 29, 2017, 7:53 AM PST), http://www.csoonline.com/article/3186225/leadership-management/black-hat-hackers-more-daring-and-experienced-than-white-hat-hackers.html [https://perma.cc/7MPR-LZL4] ("Many of the 'white-hats' I know are former grey or black hats. As such trying to put people in buckets like this is hard.").

[282] It should be noted that the United States is not alone in threatening ethical hackers. *See, e.g.*, Adnan Farooqui, *Hungarian Teen Discovers Major Security Flaw, Gets Arrested*, UBERGIZMO (July 25, 2017, 10:33 PST), http://www.ubergizmo.com/2017/07/hungarian-teen-discovers-major-security-flaw-gets-arrested/ [https://perma.cc/S5EQ-SKDW].

[283] It should be noted that Hutchins may have created and distributed malware unrelated to WannaCry before stopping that attack, though members of the security community contest that. *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/7CPY-NZHV];; Rachel Greenspan, *A Black Hat Hacker that Changed His Colour*, GLOBE & MAIL (Mar. 25, 2017), https://www.theglobeandmail.com/report-on-business/a-black-hat-hacker-that-changed-his-colour/article21305337/ [https://perma.cc/9DUE-LTBX]; Aidan Knowles, *How Black Hats and White Hats Collaborate to Be Successful*, SECURITYINTELLIGENCE (May 4, 2016), https://securityintelligence.com/how-black-hats-and-white-hats-collaborate-to-be-successful/ [https://perma.cc/JE9E-4TDC]; Greenberg, *supra* note 91.

[284] Dan Goodin, *Defeating Apple's Touch ID: It's Easier than You May Think*, ARS TECHNICA (Sept. 23, 2013, 2:00 PM), https://arstechnica.com/information-technology/2013/09/defeating-apples-touch-id-its-easier-than-you-may-think/ [https://perma.cc/4XUH-7PU7].

[285] Dan Goodin, *Fingerprint Lock in Samsung Galaxy 5 Easily Defeated by Whitehat Hackers*, ARSTECHNICA (Apr. 15, 2014, 11:52 AM), https://arstechnica.com/

2. Hiddenness Is Less Valuable than Flexibility in the Face of Repetitive Attack

Hiddenness is an asset when defenses are unique or attacks are infrequent. In general, security systems can be assessed in terms of the number of attempts an attacker is likely to make, what information an attacker gains with each attempt, and whether a community of attackers exists to communicate knowledge.[286]

To sketch a crude example of the continuum, consider the value of a covered hole, a machine gun nest, and a wall in relation to their hiddenness.[287]A covered hole is likely to trap rushing troops only once. Its very success relies on hiddenness that, by definition, will be removed once it is triggered. It cannot defeat multiple waves of attackers.[288] A machine gun nest may repel a few waves of attackers, so while its hiddenness may contribute to success in the short term, it will either be moved or overrun in the face of repeated waves of attack.[289] A wall has very little hiddenness, but in theory it may continue to survive attacks if it is monitored and maintained, being rebuilt as enemies attempt to tear it down. If an opening forms in the wall, it is critical that the defenders learn of and repair the breach before attackers can storm through.[290]

In the context of network security in a climate of global cyberwarfare, it is anticipated that attackers will be relentless, will seek to glean information from each attempt, and will communicate their findings to others.[291] An encryption scheme must resist innumerable attempts at decryption. In such an environment, adaptability, rather than static secrecy, is more likely to yield positive results. Vulnerabilities may be uncovered in many ways by many actors. Because any one mechanism is likely to fail, risk management requires a design involving multiple layers of security.[292] To continue the wall metaphor, what is needed is walls within walls, such that the

---

information-technology/2014/04/fingerprint-lock-in-samsung-galaxy-5-easily-defeated-by-whitehat-hackers/ [https://perma.cc/XT4A-4JWW].

[286] *See* Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J. TELECOMM. & HIGH TECH. L. 163, 176 (2004).

[287] *Id.* at 176–78.

[288] *Id.* at 176.

[289] *Id.* at 177.

[290] *Id.* at 180.

[291] *Id.* at 179–80.

[292] "Built-in mechanisms should be designed into the system to compensate for these failures. Layers in this context include, but are not limited to, technologies, operations, procedures and policies. Protecting the perimeter alone is never sufficient protection. The perimeter is merely a part of the holistic security approach." HURSTI, *supra* note 5, at 2.

defeat of one does not yield the defeat of the entire system. Provided those vulnerabilities are timely addressed, the system may grow and survive to continue providing security.

That is not to say that secrecy need be totally abandoned. The release of secret information such as a passcode would likely help attackers more than defenders. While public disclosure of information may be a necessary motivation for change, reasonable private disclosure is preferable.[293]

3. The Desirability of Responsible Disclosure

It is of course obvious that a system is stronger when defenders learn of vulnerabilities before attackers, are motivated to address vulnerabilities, and are able to communicate with each other to learn of additional potential vulnerabilities. While community vigilance is needed to address the first issue, incentivizing disclosure is a necessary component of the latter two. The system cannot function if disclosure does not occur, does not trigger adjustment, or is so rapid as to invite mischief before adjustments can be made.

Clearly, disclosure cannot occur if research into vulnerabilities is chilled. Thankfully, there are systematic features that naturally encourage academics and white-hat hackers to disclose their findings, provided that penalties for disclosure are absent. Academics are likely to disclose their findings to colleagues as part of the research cycle. White-hat hackers are likely to disclose their findings to the public for community recognition or altruistic reasons. These groups need only be protected from legal threats in order to propagate discoveries. The modification of the Section 1201(a)(1) anticircumvention statute serves this purpose. As noted above, grey hat hackers are likely to disclose for payment.

While the U.S. government has hidden and stockpiled vulnerabilities, it is still possible that adversaries will discover these vulnerabilities.[294] A RAND study found that "[e]xploits and their underlying vulnerabilities have a rather long average life expectancy (6.9 years)."[295] However, "[f]or a given stockpile of . . . vulnerabilities, after a year, approximately 5.7 percent have been discovered by an outside entity."[296] Accordingly, the

---

[293] Swire, *supra* note 286, at 191.

[294] LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS: THE LIFE AND TIMES OF ZERO-DAY VULNERABILITIES AND THEIR EXPLOITS, at x (RAND Corp., 2017).

[295] *Id.*

[296] *Id.*

government should err on the side of disclosure. Indeed, the government's failure to disclose vulnerabilities contributed to the success of WannaCry, Petya,[297] and other malware.[298]

The difficulty, however, is that the lead-time vendors may need to address vulnerabilities so that public disclosure does not give information to attackers and provide additional opportunity for intrusion. RAND found that "[o]nce an exploitable vulnerability has been found, time to develop a fully functioning exploit is relatively fast, with a median time of [twenty-two] days."[299] There are prominent examples of the damage that can be done due to premature disclosure, as occurred in the heartbleed leak.[300] On the whole, however, it appears that non-disclosure or unmotivated vendors[301] pose a much greater threat as vulnerabilities will not be addressed in the time before full attack.[302]

The consistent complaint of researchers is that vendors may be difficult to reach and may react antagonistically. Accordingly, the government also must establish itself as a recommended intermediary in security vulnerability disclosures. The US-CERT should establish a clearinghouse to facilitate disclosure. Individuals with knowledge of a vulnerability could report that vulnerability directly to US-CERT, which would then assume the responsibility of notifying the target vendor. While such a clearinghouse would be redundant for vendors that actively solicit bug reports, it would be beneficial to standardize methods of disclosure. Moreover, should disclosing parties wish to attract community praise, the clearinghouse could offer recognition opportunities such as accolades and leaderboards. Governmental review of vulnerabilities may also help clarify responsible disclosure

---

297 Newman, *supra* note 86.

298 Kafeine, *Adylkuzz Cryptocurrency Mining Malware Spreading for Weeks Via EternalBlue/DoublePulsar*, PROOFPOINT (May 15, 2017), https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar [https://perma.cc/65M6-NVDP].

299 ABLON & BOGART, *supra* note 294, at xiii.

300 Ben Grubb, *Heartbleed Disclosure Timeline: Who Knew What and When*, SYDNEY MORNING HERALD (Apr. 15, 2014, 4:16 PM), http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140414-zqurk.html [https://perma.cc/8TQS-GZDF].

301 Ming Yi Ang & Asankhaya Sharma, *Un-patched for Months, Could Cisco 0-day Lead to Another Round of WannaCry?*, SOURCECLEAR (May 25, 2017), https://www.sourceclear.com/blog/Un-patched-for-months-could-Cisco-0-day-lead-to-another-round-of-WannaCry—-SourceClear/ [https://perma.cc/SMD4-SXCR] (noting that an exploit similar to EternalBlue, Cisco 0-Day, CVE-2017-3881, was not patched until 61 days after it was leaked by Wikileaks).

302 HEWLETT PACKARD ENTERPRISE, HPE SECURITY RESEARCH: CYBER RISK REPORT 2015 62–63 (2015), http://h20195.www2.hpe.com/V4/getpdf.aspx/4aa5-0858enn [https://perma.cc/6NSQ-QMXF].

protocols "by interfacing between researcher and vendor on metrics like severity, likelihood of exploitation, and impact to the vendor's business"[303] and threats to critical infrastructure. A standardized disclosure timeline may result from such collaboration.

D. National Security Advantages Attendant to the Proposal

1. Increase National Security by Removing Chill and Creating Additional Incentives for Ethical Hackers

This article's proposal would strengthen national security by withdrawing a regulatory chill on needed encryption and security research. Facilitating academic publishing will broaden the scope of knowledge and stimulate additional investigation by valuable actors, while at the same time aligning with other constitutional principles of the free flow of ideas.[304] Removing the current independent anticircumvention sections of Section 1201 also would increase security by allowing white-hat tinkerers to discover existing vulnerabilities or to detect intrusions.

For example, if Russian hackers had been successful in hacking voting machine manufacturers to preload malware in voting machines, allowing review of software might discover such a practice. This scenario is not at all far-fetched, as Russians did in fact penetrate some manufacturers.[305] In a related vein, the systematic cheating of the emissions standard by Volkswagen would have likely been discovered by gearhead modders if only they had the ability to legally explore their own car software.[306]

Ideally, vulnerabilities will be detected and patched before exploits are created. It is foolish to believe, however, that defenders will always be ahead of the curve. Instead, we need a robust population of defenders to observe and react to possibly altered systems to limit the damage caused by intrusions.

2. Greater Institutional Coherence

The proposal also addresses the odd hypocrisy of national actors imploring ethical hackers and security

---

303 Klein, *supra* note 5.
304 *See supra* Section III.D.2.
305 *See supra* Section I.A.1.
306 *See infra* notes 324–328.

researchers to assist while at the same time offering vendors the tools to chill those allies. It makes little sense for the government to remove oversight of encryption publications by relaxing export controls but to also empower third parties to police those very same publications on copyright grounds. The institutional incoherence is demonstrated by the NTIA insisting that the Copyright Office is unqualified to take up national security concerns, while at the same time the Copyright Office is compelled to limit exemptions in the face of those very same concerns.[307] Limiting DMCA anticircumvention to underlying acts of copyright infringement will free the Copyright Office of the burden of weighing impacts best assessed by other agencies.

3. Greater Vendor Motivation to Address Vulnerabilities

Vendors have repeatedly demonstrated a willingness to attack researchers rather than acknowledge and address vulnerabilities. By removing a judicial lever and creating the option for governmental mediation, vendors will be more motivated to address vulnerabilities in an expeditious manner. Standardizing the vulnerability process will also allow vendors to build up necessary experience in confronting vulnerabilities discovered by third parties.[308]

4. Financial Benefits by Preventing Loss Attendant to Attacks

The cost of cyberattacks is staggering. While ransoms paid to recover data represent dramatic examples of economic loss,[309] the bulk of economic harm is caused by lost productivity during downtime. Distributed Denial of Service (DDoS) attacks

---

[307] *See supra* Section III.B.2.

[308] *See supra* Section III.D.2.

[309] A wave of ransomware attacks against hospitals generated a great deal of press coverage in 2016. *Hospitals Are Hit with 88% of All Ransomware Attacks*, BECKER'S HOSPITAL REV. (July 27, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html [https://perma.cc/G5UG-WX3J]; Keith Wagstaff, *Big Paydays Force Hospitals to Prepare for Ransomware Attacks*, NBC NEWS (Apr. 23, 2016, 6:06 AM EST), http://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176 [https://perma.cc/8WFP-KGCM] (describing the high-profile attack that was settled for a ransom of $17,000, though cost to consumer confidence and network infrastructure was likely much higher); Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 3, 2016 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ [http://perma.cc/WD9D-EHJR].

against businesses typically cost $40,000 per hour, with most attacks lasting longer than six hours.[310] The massive DDoS attack in 2016, which brought down "The *New York Times*, Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, EA, and the PlayStation network," occasioned further analysis of downtime costs.[311] The average cost to businesses was estimated at a staggering $22,000 *per minute.* [312]

This article's proposal will encourage researchers to address vulnerabilities, thereby diminishing the effectiveness of attacks. This can be accomplished on two fronts, by strengthening consumer-side devices and by lowering the number of bots available for mass DDoS attacks against service providers.

5. Encouraging STEM Education

This proposal will further Science, Technology, Engineering, and Mathematics (STEM) education by broadening the resources available for research, by elevating the status of white-hat hackers, and by increasing opportunities for young persons to engage in ethical hacking. Ethical hacking has been recognized as an effective means of recruiting student interest[313] and imparting necessary security skills.[314] These opinions are largely reflected in the comments of the Association of American Universities, the American

---

[310] TIM MATTHEWS, INCAPSULA SURVEY: WHAT DDOS ATTACKS REALLY COST BUSINESSES 6 (2014), https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf [https://perma.cc/5H4Z-UTKJ].

[311] Robinson Meyer & Adrienne LaFrance, *When the Entire Internet Seems to Break at Once*, ATLANTIC (Oct. 21, 2016), https://www.theatlantic.com/technology/archive/2016/10/when-the-entire-internet-seems-to-break-at-once/504956/ [https://perma.cc/H2GY-32PM].

[312] CYBER SECURITY ON THE OFFENSE: A STUDY OF IT SECURITY EXPERTS, PONEMON INSTITUTE 5 (Nov. 2012), https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf [https://perma.cc/BNV6-YTZK].

[313] Joe Gervais, *Hack Away, Kid: How Schools Can Teach Students to Become Ethical Hackers (and Protect Their Systems in the Process)*, SLATE (May 11, 2015, 9:18 AM), http://www.slate.com/articles/technology/future_tense/2015/05/schools_should_teach_students_to_be_ethical_hackers.html [https://perma.cc/93W9-2AT6]; Steve Morgan, *Hacker High School Teaches Cyber Security Skills to Teens*, FORBES (Mar. 20, 2016, 8:23 AM), https://www.forbes.com/sites/stevemorgan/2016/03/20/hacker-high-school-teaches-cyber-security-skills-to-teens/#3cb65d154d50 [https://perma.cc/ES86-E6BT]; Mariya Pylayev, *H.S. Cyber Security Program Aims to Recruit Girls, Minorities with Fun, Ethical Hacking Skills*, AOL NEWS (Feb. 3, 2014, 12:00 PM), https://www.aol.com/2014/02/03/stem-cyber-security-program-girls-minorities-ethical-hacking/ [https://perma.cc/BEV9-XCKH].

[314] Regina D. Hartley, *Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack*, 24 J. INT'L TECH. & INFO. MGMT. 95, 101 (2015) (collecting research and noting that "thinking like a hacker and acting like an 'ethical hacker' is a critical skill for a successful career in security for web applications").

Council on Education, the Association of Public and Land-Grant Universities, and Educause, which continue to hope for "[S]ection 1201 liability [limited] to circumvention only where the act of circumvention results in infringement" as currently Section 1201 is "inherently prejudicial to innovative educational approaches."[315]

V. CRITICISMS AND AREAS FOR FUTURE RESEARCH

The likely criticisms of this article's proposal center on its feasibility, the adequacy of the current review process, and the proposal's overall impact on safety.

A. Change of the DMCA Is Unfeasible in Light of Stakeholder Power and Treaty Obligations

A potential criticism of the proposed approach is that it is simply not feasible in light of powerful rights-holders' concerns and World Intellectual Property Organization (WIPO) treaty requirements.[316] Critics would rightly point to the failure of recent attempts to address these issues legislatively: for example, H.R. 1587: Unlocking Technology Act of 2015[317] and H.R. 1883: Breaking Down Barriers to Innovation Act of 2015[318] never made it out of committee, though each proposed somewhat similar solutions to the first plank of the proposal.

While there are powerful interests combating the outright removal of Section 1201, the recent failures did not occur in the backdrop of foundational attacks against the electoral integrity of the Republic or national hospital networks. The recent spate of exemptions, along with critical governmental reports, demonstrates a newfound awareness of institutional actors that may facilitate change.[319] The sobering results of voter machine hacking, along with a strong reaction

---

[315] The Association of American Universities, the American Council on Education, The Association of Public and Land-Grant Universities, and Educause, Comment Letter on Section 1201 of the Digital Millennium Copyright Act—Sixth Triennial DMCA Rulemaking 3, 6 (Mar. 27, 2015), https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Intellectual%20Property/EDU-AAU-ACE-APLU-Comment-SEC-1201-DMCA_2016.pdf [https://perma.cc/WM9H-ELNJ].

[316] Samuelson, *supra* note 147, at 370–71.

[317] Unlocking Technology Act of 2015, H.R.1587, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1587?q=H.R.+%201587 [https://perma.cc/BF2V-B73X].

[318] Breaking Down Barriers to Innovation Act of 2015, H.R. 1883, 114th Cong. (2015), https://www.govtrack.us/congress/bills/114/hr1883 [https://perma.cc/BKD6-9WJQ].

[319] *See supra* Section III.B.

to foreign meddling in American electoral systems, may create a more amenable environment.

As to the requirements of WIPO, notwithstanding the grandiose statements during DMCA's drafting, there is nothing in the treaty that obligates barring the act of circumvention attendant to lawful activities.[320] WIPO requirements could be, and indeed are, satisfied by interpretations of an anticircumvention right that is dependent on underlying copyrights.[321]

B. Incremental Progress in Triennial Review Is Measured and Responsive

Proponents of the DMCA may also argue that the granting of specific exemptions is a more measured approach. In the face of likely resistance to wholesale change of the DMCA, critics of the proposal could point to the triennial process as an effective way to adapt to a changing technological environment while respecting the rights of rights holders.

This criticism ignores the long lag in the review process, the inherently arbitrary nature of exemptions, and the failure to inspire research that may rely on re-criminalized activity at the expiration of the exemption. The current exemption for good faith security researchers may represent a small step in the right direction, though it has several troubling limitations, not least of which is that it must be renewed every three years.

Most troubling is that the exemption process appears to be reactive, waiting for initial threats to spill over into real-world consequences before easing research restrictions. This pattern is evident from the recent exemption regarding exploring software used in motor vehicles and consumer products.

The motor vehicle exemption appears to have been motivated by a demonstration by researchers of a vulnerability that hackers could use to wirelessly car jack and potentially kill a moving vehicle. In this case, researchers remotely commandeered and killed a Jeep travelling on the freeway. Specifically, "the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers . . . [before] cut[ting]

---

[320] Jonathan Band & Taro Isshiki, *The New Anti-Circumvention Provision in the Copyright Act: A Flawed First Step*, 3 No. 11 CYBERSPACE L. 2 (1999) (explaining that the DMCA's anticircumvention regulations were not required for compliance with the WIPO Copyright Treaty); Samuelson, *supra* note 180 at 537 ("Administration officials admitted in Congressional testimony that its preferred legislation went beyond what the WIPO Copyright Treaty required."). *See generally* Samuelson, *supra* note 147 (discussing the negotiations leading to conclusion of the WIPO Copyright Treaty).

[321] Samuelson, *supra* note 147, at 409–13.

the transmission."[322] The vulnerability was present in cars that had the "Sprint-powered Uconnect feature and . . . 8.4-inch touchscreen systems. . . . includ[ing] Ram, Cherokee, Grand Cherokee, Durango, Viper, Challenger, and Chrysler models."[323] The revelation caused the recall of over one million cars and prompted outcry for a DMCA exception.

The Volkswagen emissions fraud, commonly known as Dieselgate, may also have helped the proposed exemption. Volkswagen, in an effort to appear to meet emissions standards on their "clean diesel" line—cars with turbocharged direct injection (TDI) diesel engines—programmed their cars to trigger a low-performance, low-emissions mode only during laboratory emissions testing.[324] The software would recognize a testing condition through "the position of the steering wheel, vehicle speed, the duration of the engine's operation, and barometric pressure." [325] The software would then trigger the artificially low emissions mode.[326] The effects of the software were noticed when researchers discovered a large discrepancy between their road emissions tests and laboratory tests. As part of a plea deal, Volkswagen was ordered "to pay a $2.8 billion criminal fine for rigging diesel-powered vehicles to cheat on government emissions tests."[327] The Electronic Frontier Foundation correctly noted that had gearhead hackers been allowed to investigate the software on their own cars, Volkswagen's deceit would have been uncovered much sooner.[328]

---

[322] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/5E9B-URUH]; Sharon Shea, *Alleged Car Hack Prompts Call for Vehicle Security Act, DMCA Exemption*, TECHTARGET (July 24, 2015), http://searchsecurity.techtarget.com/news/4500250530/Alleged-car-hack-prompts-call-for-vehicle-security-act-DMCA-exemption [https://perma.cc/CYJ8-UDWL].

[323] Eduard Kovacs, *Feedback Friday: Industry Reactions to Remote Car Hacking*, SECURITYWEEK (July 24, 2015), http://www.securityweek.com/feedback-friday-industry-reactions-remote-car-hacking [https://perma.cc/3DYE-4GGQ].

[324] James Grimmelmann, *The VW Scandal Is Just the Beginning*, MOTHERJONES (Sept. 24, 2015, 10:00 AM), http://www.motherjones.com/environment/2015/09/volkswagen-defeat-device-copyright-harry-potter/ [https://perma.cc/F7ER-HPWU].

[325] *Id.*

[326] *Id.*

[327] Christina Rogers & Mike Spector, *Judge Slaps VW with $2.8 Billion Criminal Fine in Emissions Fraud*, WALL ST. J. (Apr. 21, 2017, 1:37 PM ET), https://www.wsj.com/articles/judge-slaps-vw-with-2-8-billion-criminal-fine-in-emissions-fraud-1492789096 [https://perma.cc/K8Z2-VGX4].

[328] Kit Walsh, *Researchers Could Have Uncovered Volkswagen's Emissions Cheat if Not Hindered by the DMCA*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Sept. 21, 2015), https://www.eff.org/deeplinks/2015/09/researchers-could-have-uncovered-volkswagens-emissions-cheat-if-not-hindered-dmca [https://perma.cc/7ZWJ-ML63].

The exemption for investigation of consumer goods was likely tied to the rise of malware infecting and enslaving consumer products. Hackers then directed these devices to unleash enormous waves of traffic to overwhelm servers and cause outages. The occurrence of huge botnets[329] made up primarily of poorly defended internet-connected consumer goods (so-called Internet-of-Things Botnets) is an enormous security threat, as 2015 saw an increasing wave of DDoS attacks from infected devices. Earlier that year, the first IoT botnet made up primarily of infected routers was reported and attributed to the LizardStresser botnet.[330]

Unfortunately, the exemption was subject to a one-year delay, during which time the size and strength of IoT botnets only grew. In October 2016,[331] a widespread DDoS attack[332] was launched against Dyn, a manager of the DNS network.[333] This brought down "Twitter, the Guardian, Netflix, Reddit, [and] CNN, [among] others in Europe and the United States."[334] Commentators noted that "hundreds of thousands of websites became unreachable"[335] and that "half the internet shut down."[336] The attack was the largest of its kind, involving

---

[329] A botnet is composed of bots. Bots or zombies are enslaved devices that act in concert to achieve a purpose. Brett Stone-Gross et al., *Your Botnet is My Botnet: Analysis of A Botnet Takeover*, PROCEEDINGS OF THE 16TH ACM CONFERENCE ON COMPUTER & COMMUNICATIONS SECURITY (2009), https://www.fbiic.gov/public/2009/may/torpig.pdf [https://perma.cc/FTR5-MEU9]; Nick Clayton, *Where to Rent a Botnet for $2 an Hour or Buy One for $700*, WALL ST. J. (Nov. 5, 2012, 9:43 AM GMT), http://blogs.wsj.com/tech-europe/2012/11/05/where-to-rent-a-botnet-for-2-an-hour-or-buy-one-for-700/ [https://perma.cc/TA8L-V9WG].

[330] Tom Spring, *LizardStresser IoT Botnet Part of 400Gbps DDoS Attacks*, THREATPOST (June 30, 2016, 7:00 PM), https://threatpost.com/lizardstresser-iot-botnet-part-of-400gbps-ddos-attacks/119006/ [https://perma.cc/M75G-ZXYA].

[331] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, ALERT-TA16-288A, HEIGHTENED DDOS THREAT POSED BY MIRAI AND OTHER BOTNETS (Oct. 17, 2017), https://www.us-cert.gov/ncas/alerts/TA16-288A [https://perma.cc/DW3T-GGDE].

[332] Michael Kan, *DDoS Attack on Dyn Came from 100,000 Infected Devices*, COMPUTERWORLD (Oct. 26, 2016, 2:21 PM PT), http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html [https://perma.cc/63B2-TBS7] (noting that attack originated from 100,000 infected devices).

[333] Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, DYN (Oct. 26, 2016), http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ [https://perma.cc/H4QX-4KD2].

[334] Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016, 16:42 EDT), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [https://perma.cc/GN89-JQVK].

[335] Daniel Smith, *How Friday's Massive DDoS Attack on the U.S. Happened*, RADWARE, (Oct. 23, 2016), https://blog.radware.com/security/2016/10/fridays-massive-ddos-attack-u-s-happened/ [https://perma.cc/2QHV-7L8D].

[336] William Turton, *This Is Why Half the Internet Shut Down Today*, GIZMODO (Oct. 21, 2016, 8:36 AM), http://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835 [https://perma.cc/X983-ZVWA].

primarily-IoT Botnet Mirai traffic of 1.2 terabytes per second.[337] Numerous industry sectors have noted their vulnerability to DDoS attacks, characterizing the Dyn attack as a "practice run" by hackers[338] and predicted that 2017 would see even more DDoS attacks.[339] It is a sad state of affairs when defenders are constrained until initially successful attacks are discovered.

C. Encouraging Malicious Hacking

Critics may argue that the relaxation of Section 1201 will encourage hacking by malicious actors, erasing any gains accrued through greater academic openness. Of course, the larger question of the impact of academic openness always warrants further study. This specific argument, however, reflects two fundamental misunderstandings: (1) the belief that malicious hackers are somehow dissuaded by DMCA penalties, and (2) a security through obscurity position that is untenable in the digital world. Malicious hackers, especially those employed by foreign governments, are not known to be very responsive to domestic laws. It should be assumed that underlying vulnerabilities will eventually be discovered—no systems are truly secret—so we must not constrain defenders, even at the risk of marginally incentivizing attackers.

CONCLUSION

While IP law is not often thought of in terms of national security, the acute cyberwarfare climate requires a reexamination of laws constraining the public's role in national defense. The DMCA has continued a deleterious trend of inviting governmental regulation of needed encryption and security research, inherited from a century-old doctrine originally concerned with biplanes and propeller-mounted machine guns. This security through obscurity approach must be abandoned. By removing independent anticircumvention provisions while encouraging greater communication between the security community and product vendors, we will harness the energy of researchers and altruistic hackers alike. In the

---

[337] Hilton, *supra* note 333.

[338] JAMES SCOTT & DREW SPANIEL, RISE OF THE MACHINES: THE DYN ATTACK WAS JUST A PRACTICE RUN, INST. FOR CRITICAL INFRASTRUCTURE TECH. (Dec. 2016), http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf [https://perma.cc/Z5K4-HT64].

[339] Maarten van Horenbeeck, *2017 Predictions: US Isolationism, DDoS, Data Sharing*, ITPROPORTAL (Dec. 29, 2016), http://www.itproportal.com/features/2017-predictions-us-isolationism-ddos-data-sharing/ [https://perma.cc/7M4Q-5PT2].

face of unprecedented attacks, we must not mistake a veil of secrecy as a wall of security nor imagine that our vulnerabilities will disappear provided we keep our eyes shut.