

Digital Alienation

Nico Hailey

June 8, 2003

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

...

(A) to “circumvent a technological measure” means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner;

—Excerpt from the Digital Millennium Copyright Act, sec. 1201.
Circumvention of copyright protection systems

A bad system design is secure as long as the details remain secret, but quickly breaks once they are released. A good system design is secure even if the details are public.

– Bruce Schneier, *Secrets & Lies*, page 344

1 Introduction: Why Do Cryptographers Care About US Copyright Laws?

Five years after the Digital Millennium Copyright Act passed, we are still trying to deal with its repercussions. One need not be a Derrida scholar to see that the most cursory of critical discourses immediately problematizes the “anti-circumvention” provision of the DMCA in several ways. The most pressing issue for the many of the security community is the legal bludgeoning of several prominent Researchers. The meta-issue is the freedom of research bodies to self-determination, unfettered by corporate interests and politicians bought with ignorance and fear. The DMCA and security research woes are but a symptom of this meta-issue, played out in courts, conferences, and universities.

The core of copyright is Intellectual Property (IP). It is a basis of our economy to protect the copyright holders from the unwashed masses. This is not

the section of the DMCA which sends many into phantasmic spasms. There is no reason to treat digital objects any differently than how non-digital objects are currently treated. Problem areas arise when the legal system specifies the computational machinery for copyright enforcement in the mutable world of digital objects. The word “encryption” seems to be reflexively encrypted. Some think it decrypts to an inviolate black box, standing up for the good and pure rights of American corporate IP. While to others, “encryption” is cryptography, a vibrant research field of challenging puzzles. Mr. Heston of the National Rifle Association tirelessly told us “guns don’t kill people, people kill people”: similarly, decryption doesn’t pirate DVDs, people pirate DVDs.

Security researchers generally go beyond what a naive lawyer would consider fair use. The naive lawyer is fairly unaware of the tasks involved in security research. Reverse engineering and breaking an encryption scheme require somewhat broader powers than simply making a back-up copy of the copyrighted material (in case of drive failure, break glass). By legislating against tools and algorithms, instead of malicious acts, the law is entering a morass devoid of intent and the assumption of innocent until proven guilty. The DMCA also sets up a few tidy paradoxes. For instance, it states that reverse engineering is not prohibited, but later it introduced the anti-circumvention section. This leaves the culpability of the citizenry resting on the whim of particular judges and prosecutors with few assurances of consistency.

Using an infinity key, which analyzed and opened all forms of locks known, he entered Polokov’s apartment, laser beam in hand.
–Philip K. Dick, *Do Androids Dream of Electric Sheep*, p. 88

2 First Up Against the Wall When the Revolution Came[DNA RIP]: or, please turn your infinity keys in at the front desk.

Algorithms and tools have no moral alignment. There is rarely a tool, even in the dens of hats of darkest midnight, which cannot be used by forces of law and order. Both security and law depend on a negotiated understanding of a morality. Forming a morality entails precise definitions. All bodies participating in this morality need to speak similar languages, so they can at least pretend to find meaning in their common words. Here are the pertinent building blocks for moral definitions for the rest of this paper¹.

Legal/Illegal is the known state of legality or illegality, precluding the anti-circumvention provision of the DMCA. This definition holds for the duration of the rest of the morality definitions. It is thusly restricted to ease classification of the players in the DMCA game.

¹Attempts have been made to define sweeping generalizations and use them in a context which is consistent with the literature.

Feds are US federal agents, obviously White Hat.

White Hats are the researchers, including independent, academic and corporate. They believe in the policy of full-disclosure [2]. This policy states that researchers should tell the world what they know. The tools of the White Hats can be used legally or illegally. They, and their products, are not biased to illegal users or tasks. White Hats are fundamentally motivated and committed to advancing the state of the art for the benefit and protection of all.

The Grey Hats are the people who, while their tools may have features which seem biased to the illegal, they themselves, have broken no laws. They are simply providing these controversial tools as proof-of-concept or for user education. If someone uses a Grey Hat tool for illegal purposes, they invoke the NRA's defense. Grey Hats have frequently been seen floating in a directionless moral void.

The Black Hats are the people who intentionally, knowingly, or maliciously steal IP for fun and/or profit. These people are guilty regardless of their violation of the anti-circumvention clause. They tend to redistribute stolen IP en masse. Strangely enough, this was illegal before the DMCA was signed into law.

The term Researchers is used to refer to White and Grey Hat aligned researchers. Research as defined by [15]:

- 1.) careful or diligent search.
- 2.) studious inquiry or examination; especially : investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws.
- 3.) the collecting of information about a particular subject.

A premise of this paper is that the anti-circumvention provision of the DMCA is an inconsistent law which violates previous copyright cannon. Hence, I argue that there exist no Black Hat Researchers (with the above standardly accepted value of "research") in the US Security Community in the context of the DMCA.

The Security Community is everyone involved in computer security who expresses his opinion in some tangible way: books, blogs, mailing lists, Usenet, webboard posting, interviews, IRC, conferences, email, television, etc. The Security Community Zeitgeist is formed from this chatter. In this context, it crystallizes around legal issues which threaten its existence and meme nexus. This paper refers to Security Community meme nexus as those places, virtual or real, which act as an interactive common carrier for Security Community memes². In McLuhanian terms, it is this environment which the storm of the DMCA has turned into an "object of attention" [3]. This anti-environment is dutifully opening "the door of perception to people otherwise numbed in

²Examples of meme nexus are: slashdot.org, USENIX, securityfocus.com, eff.org, nanog, cypherpunks, 2600, defcon.org, ACM journals, IEEE journals...

a nonperceivable situation”. These people are the cellular machinery of the gestalt, when the cells are attacked the previously nonperceivable is the new cause celebre. In our democracy, motivation of subcultures has legal relevance since it builds biomass at protests, conferences and the polls.

This sociological consequences of the DMCA in the Security Community warrants as much notice as the technological and legal challenges. On this axis, belongs the illegible damage. Damage, which is not discernible from solely the legal dockets. Illegible damage is the restriction of Researcher’s agency with threats of dire legal repercussions, including financial hardship and jail. This agency restriction is manifest via: Researchers refusing to attend US technical conferences (boycott) [7]; pulling their research from publication under duress (intimidation) [13]; removing their tools out of fear of prosecution without prompting(self-censorship) [12]; meme nexus meme reduction(forced link removal), fatigue and intimidation [14].

For the most banal event to become an adventure, you must (and this is enough) begin to recount it.
– JP Sartre, Nausea, p 39

3 Full Disclosure

These individual and community high levels of paranoia weaken the security of all computing systems because they are legally precluded from full disclosure[n schnier]. Historically, in full disclosure, when a vulnerability in a system is found, the vendor is contacted, given time to issue a patch, and then the patch and the vulnerability are published at around the same time. This is both polite and motivational to the vendor. It is polite since it gives the vendor a grace period to fix the issue. Motivational, because if the vendor fails to issue a fix, then the world knows that the vendor callously sells insecure software. The Security Community is then given the chance to make a patch themselves (on open systems), or engineer a work-around based on exact knowledge of the vulnerability. Under the DMCA, this can be illegal.

Thief in the Shadows!... My armor is like tenfold shields, my teeth are swords, my claws spears, the shock of my tail a thunderbolt, my wings a hurricane, and my breath death!
– Smaug to Bilbo, p 216, The Hobbit, J.R.R. Tolkien

4 Threats: HP/snosoft July 2002, MS/slashdot May 2000

In July, 2002, HP used the DMCA to threaten snosoft.com for an releasing exploit code to a vulnerability (which had been known and unpatched for a

year) via the Security Community nexus Buqtraq [11]. However, in this case, the agency of the security community zeitgeist outweighed the DMCA based intimidation and HP dropped the threat [16].

In May of 2000, meme nexus slashdot.org posted an article about Microsoft embracing and extending the supposedly open Kerberos protocol used in the authentication scheme for Windows 2000. This was the first time Microsoft offered network operating system authentication services which employed more than trivial encryption technology [4]. Microsoft appeared to have altered Kerberos in subtle, but sufficient, ways to assure Windows 2000 Kerberos-based domain controllers would not inter-operate easily with the open standards of public domain Kerberos. Naturally, in comment-land on Slashdot, the opinionated and prolific members engaged in a rigorous technical discussion of the MS version of Kerberos. One member did not particularly care to follow the End User License Agreement (EULA) which MS enforced upon those who desired to see MS's non-standard implementation of Kerberos. This user chose to express his viewpoint on MS, the MS EULA, and the MS modifications to Kerberos via posting, in entirety, the MS Kerberos code to Slashdot (this code was available for free-like-beer from MS, but covered by the EULA, which meant it was not free-like-speech) [6]. MS responded with a DMCA suit threat coupled with the demand that the controversial comment be removed [5]. Slashdot responded that it was in the common carrier business, not the censorship business. Three years later, the controversial post remains searchable and accessible on Slashdot.

Go straight for the jugular. Get right into felonies. The mentality of Las Vegas is so grossly atavistic that a really massive crime often slips by unrecognized.

– page 173, Fear and Loathing in Las Vegas, Hunter S. Thompson

5 Trial: Sklyarov, Adobe, and Elcomsoft – July 2001

The initially polarizing DMCA case was that of Elcomsoft, a Russian company, and more specifically Dimitry Sklyarov, a Russian PhD student. Sklyarov was arrested after presenting his research on the security of Adobe's e-book format at Defcon 9 (2001) in Las Vegas. It seems pertinent to the selective enforcement and conflicted wording concerns on the DMCA to note that: Sklyarov is a Russian national; Adobe is an American High Tech company; Defcon is a Security Community nexus, which historically has been treated like the DMZ between the Feds, the Researchers, Security Community members and the Black Hats³;

³In fact, when this author attended Defcon 8 (2000) there were multiple Fed led panels, systems and security administrators and researchers from all over industry and academia, as well as Black Hats. However the media regularly refers to this unusual body of Security Community members as "Hackers". The word "hacker" seems to be devalued to the point of uselessness; it only provokes pedantic, tautological discussions of etymology and orthodoxy.

this was the first time Defcon was held under G.W. Bush administration. Sklyarov spent a month in jail, and three months detained in the US before being allowed to return home. Security Community members engaged in immediate nation-wide protests⁴. They were demanding Sklyarov's release and sharply critiquing the DMCA and Adobe.

Adobe promptly withdrew its support of criminal charges against Sklyarov when it issued a joint press release with the Electronic Frontier Foundation [9]. It is reasonable to speculate that Adobe did not desire the PR disaster of having respectable programmers, Security Community members, and clients target it in nation wide protests. Adobe's initial support of this measure alienated a large number of their user base. They could not afford to let such negative branding continue.

Elcomsoft's contested product provided a way to back up an e-book, a feat which was impossible to do without circumventing the e-book encryption, and thus breaking the DMCA. This was a confluence of the two major problems with the DMCA: fair use and anti-circumvention. Fair use doctrine states that a backup copy for one's own personal use is allowed [1]. This software lets an e-book user exercise their fair use rights. In fact, there were never any pirated e-books found during the trial and the e-book format never proved profitable [8]. Adobe, like HP, underestimated the ire their anti-circumvention move engendered in the Security Community and related communities (civil libertarians, general technophiles, librarians). In the acquittal stage of the criminal case, the jury commented on the fact that the DMCA is highly confusing and concluded it difficult to require that non-citizens understand the DMCA [8].

An idea that is not dangerous is unworthy of being called an idea
at all.

–Oscar Wilde

6 Self Censorship: Tom Liston; Niels Ferguson

The high profile DMCA cases are imbued with sometimes contradictory gifts and curses to the Security Community. The Sklyarov case seemed a dystopian absurdist farce to a casual observer at the time. While it considerably raised the illegible damage toll to the Security Community, it also was one of the most accessible cases to the average citizen. Copyright law is something that few feel

This word will only be used in quotes. White/Grey Hat Researchers, and Black Hats offers clearer terminology in this paper.

⁴This author attended several free-sklyarov/anti-DMCA protests at the Boston Commons. The protesters engaged in community education about Copyright Law and Fair Use via fliers, folk songs, guerilla theater, and discussion with passers by. Adobe HQ was also protested in San Jose. Adobe quickly dropped their civil suit against Sklyarov. Many of the Boston protesters were Open Source Community members, such as the Boston-centric gnome developers, who typically share a large overlap with Security Community members as a large percentage of their meme nexus are shared.

passionate about understanding, until one trespasses upon the Draconian “illegal” face of the DMCA. Unfortunately, free speech and research are restricted for the Researchers who have never directly experienced a DMCA lawsuit. The risk of a lawsuit to oneself, or to one’s upstream providers or employers is so great that individuals and bodies in murky DMCA standing have chosen to censor themselves voluntarily rather than risk the uncertainty of violation.

Niels Ferguson, on August 15, 2001, a HDCP (high bandwidth digital content protection system) researcher took down his online papers [10]. He asserts that HDCP is fatally and trivially flawed, yet he can’t operate under full disclosure principles. He is not even a US citizen, but has sufficient social and business ties to the US that facing US penalties would be an unthinkable hardship. He sites lack of Freedom of Speech, Jurisdiction, and the flawed nature of the DMCA itself as the reasons for his self-censorship.

In August of 2001, Tom Liston became a hero of the system administration community when he released LaBrea during the chaos of the first Code Red outbreak. LaBrea was innovative because it was the first White Hat tool which could DoS an attacker (worm infested machines). Like many of the worms that followed, Code Red used up as much bandwidth as it could, and spread rapidly by searching for new vulnerable machines to infect. A heavily infected LAN would saturate its link to the Internet within twenty minutes. LaBrea is a single floppy image, based on Trinitix/Linux and has an interestingly modified TCP/IP stack. It exploits the three way hand shake (it gets a SYN, responds with a SYN-ACK, and then, nevermore) and TCP/IP design for robustness to trap one machine at one connection for long periods of time. This meant that the hostile machine which attempted to attack a LaBrea machine would get trapped in the “tar-pit”. Under the new Illinois state level descendant of the federal DMCA, “disruption” of communications traffic and concealing origin of communication (part of how LaBrea works is spoofing its address to attacking machines) is a violation [12]. In February of 2003, Mr. Liston removed LaBrea from his website.

The sky above the port was the color of television, tuned to a dead channel.

– William Gibson, Neuromancer, page 1.

7 The future as it was

The future of security research regarding the DMCA and derivative legislation seems to be split upon established power/money/influence lines. Digital Rights Management issues must diverge from anti-decryption legislation for a sane legal dialog between civil-liberties-minded individuals and restrictive copyright-minded individuals to occur. Unfortunately, from the upswing in State level “Super DMCA” laws, which are all but written by the Motion Picture Assoc. of America, a sane dialog doesn’t appear to be what is wanted. Unless the US

gets a consistent grip on what the DMCA actually means and how often it is actually going to be applied, the current stultifying conditions will continue to chill research in the US or move it offshore.

Given the post-9/11 American political climate of poor risk assessment, general security paranoia by the populace at large, and deafening jingoism bathing public discourse, any attempt at relaxing “protective” laws will prove futile. There is a basic and deep cultural rift between people who are willing to sacrifice their civil liberties, piecemeal, for politician’s soothing promises of safety, and those who fear every small erosion of the Enlightenment ideals of freedom, equality, and brotherhood formalized in the U.S. Constitution and Bill of Rights.

We now have the Homeland Security Cyber Security machinations installed, as well as DARPA projects like LifeLog, and Terrorist Information Awareness. Computer security is no longer an afterthought to keep script-kiddies from posting porn on NASA’s home page. Computer security is not well enough understood by the average American, nor the majority of lawyers for the initial laws produced to be anything but confusing, biased, and possibly unconstitutional. This storm will break, eventually. This meme nexus-defined anti-environment will return to the subliminal contrivances of daily life when people realize that digital objects require the same amount of consciousness as non-digital objects. Perhaps then the hysteria on all sides will subside.

References

- [1] *Secrets and Lies*, Bruce Schneier (Wiley & Sons, 2000), page 338
- [2] *Security in Computing*, Charles P. Pfleeger, Shari Lawrence Pfleeger (Prentice Hall, 2003), page 556
- [3] http://www.tauzero.com/Brenda_Laurel/Severed_Heads/Imagery_and_Evolution.html
Last Accessed June 6th, 2003
- [4] <http://www.atstake.com/research/lc/>
Last Accessed June 6th, 2003
- [5] <http://www.tnr.com/cyberspace/cohen052300.html>
Last Accessed June 6th, 2003
- [6] <http://slashdot.org/article.pl?sid=00/05/02/158204>
Last Accessed June 6th, 2003
- [7] http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html
Last Accessed June 6th, 2003
- [8] <http://news.com.com/2100-1023-978176.html>
Last Accessed June 6th, 2003

- [9] <http://www.adobe.com/aboutadobe/pressroom/pressreleases/200107/20010723dcma.html>
Last Accessed June 6th, 2003
- [10] <http://www.macfergus.com/niels/dmca/cia.html>
Last Accessed June 6th, 2003
- [11] <http://news.com.com/2100-1023-947325.html>
Last Accessed June 6th, 2003
- [12] <http://www.hackbusters.net/>
Last Accessed June 6th, 2003
- [13] http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html
Last Accessed June 6th, 2003
- [14] <http://www.2600.com/dvd/docs/>
Last Accessed June 6th, 2003
- [15] <http://www.m-w.com/>
Last Accessed June 6th, 2003
- [16] <http://www.wired.com/news/technology/0,1282,54297,00.html>
Last Accessed June 6th, 2003