The Digital Millennium Copyright Act: A Security and Privacy Analysis

Divya Aradhya

Saint Leo University

Author Note

Contact: divya.aradhya@saintleo.edu

October 21, 2016.

Table of Contents

The Digital Millennium Copyright Act: A Security and Privacy Analysis

In 1998, the Digital Millennium Copyright Act (DMCA) updated the existing copyright law by providing the legal framework for how copyright holders make claims of copyright infringement in the digital world, given that only an Internet Service Provider (ISP) (e.g., a cable company, telephone company, college, university, etc.) has the records necessary to match an Internet Protocol (IP) address and time stamp to an individual. The DMCA tries to balance the needs of copyright holders whose digital works can be rapidly, perfectly, and infinitely copied and the liability of an ISP for its users' infringing activity, all in the context of protecting intellectual property to promote innovation. [8]

The Digital Millennium Copyright Act (DMCA) was enacted by the 105th United States Congress, signed by President Clinton, on October 28, 1998. It amended the Copyright Act of 1976 and its Long Title states: *To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.* [10]

Background and Cause for Development of the DMCA

In the 1990s there was great digital debate. With Internet and digital technology becoming available throughout the United States, copyright questions abounded.

In a course of a six-year period there was enormous discussion and debate - both in the House of Congress and among educators, librarians, content producers, publishers, and in the public at large, as to how copyright laws should be adapted to the new digital technology.

The growing opinion of people just before the drafting of the DMCA was that new technologies allowed users to freely transfer music, texts, and other works of art to other people. This was especially true of the Internet, which made downloading music, text, and movies easier than ever

before. Copyright holders felt that many of the laws currently on the books did not provide enough protections for their works in the digital realm.

As a result of these debates, the U.S. signed two treaties that offered more protections for international copyright holders and also addressed technology issues relevant to keeping copyrights safe. These treaties, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), were signed by the United States in December of 1996 and ratified by Congress. These treaties were written with the intention of extending around the world protections for copyright holders in their respective countries. [1] By 1998, the primary issues had been resolved and enacted into a statute called the Digital Millennium Copyright Act.

Major Provisions of the DMCA

According to the U.S. Copyright Office summary [2], The DMCA is divided into five titles:

- **Title I**, the "**WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998**," implements the WIPO treaties.
- **Title II**, the "**Online Copyright Infringement Liability Limitation Act**," creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.
- **Title III**, the "Computer Maintenance Competition Assurance Act," creates an exemption for making a copy of a computer program by activating a computer for purposes of maintenance or repair.
- **Title IV** contains six miscellaneous provisions, relating to the functions of the Copyright Office, distance education, the exceptions in the Copyright Act for libraries and for making ephemeral recordings, "webcasting" of sound recordings on the Internet, and the

applicability of collective bargaining agreement obligations in the case of transfers of rights in motion pictures.

- **Title V**, the "Vessel Hull Design Protection Act," creates a new form of protection for the design of vessel hulls.

Title I and Title II are the major ones and are explored below.

Title I: WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998

Title I implements the WIPO treaties. First, it makes certain technical amendments to U.S. law, in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code. [2].

- U.S. Code § 1201 - Circumvention of Copyright Protection Systems
- U.S. Code § 1202 – Copyright Management Information

  In effect Title I-
- Prohibits the "circumvention" of any effective "technological protection measure" (e.g., a password or form of encryption) used by a copyright holder to restrict access to its material
- Prohibits the manufacture of any device, or the offering of any service, primarily designed to defeat an effective "technological protection measure"
- Defers the effective date of these prohibitions for two years and 18 months, respectively
- Requires that the Librarian of Congress issue a three-year waiver from the anti-circumvention prohibition when there is evidence that the new law adversely affects or may adversely affect "fair use" and other non-infringing uses of any class of work

- Expressly states that many valuable activities based on the "fair use" doctrine (including reverse engineering, security testing, privacy protection and encryption research) will not constitute illegal "anti-circumvention"
- Makes no change to the "fair use" doctrine or to other information user privileges and rights [3]

Legal Proceedings from Application of DMCA TITLE I

Universal City Studios, Inc. v. Reimerdes, Johansen, Corley - 111 F.Supp.2d 294 (S.D.N.Y. 2000) aff'd 273 F.3d 429 (2d Cir. 2001) [4]

Universal and other movies studios used an encryption system called CSS that made so that DVDs could only be played on licensed DVD players that wouldn't allow the user to copy the data. CSS was shared with the companies that made the DVD players. Johansen was a 15-year old hacker who reverse engineered a DVD player and developed a program called DeCSS that would let users copy the data DVDs.

Universal started sending out cease and desist letter to all the web sites that allowed users to download the DeCSS code. Corley's website hosted the code, but deleted in when Universal threatened to sue. However, Corley provided links on their website to other websites that still had the code available.

Universal sued Corley for copyright infringement. Corley argued that this was a 1st Amendment freedom of speech issue because he didn't think CSS should be legal. Universal argued that this was akin to publishing the combination to a bank vault to encourage people to rob the bank.

The Trial Court found for Universal. The Trial Court looked to the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §1201(a)(2)) and found that DeCSS was a copyright violation because it's only purpose was to defeat copyright protection. Therefore offering to transfer the DeCSS

code to a user was not legal. The Court found that Corley engaged in the functional equivalent of transferring the DeCSS code to the user by linking to sites that hosted the code. Especially because many of the sites Corley linked to had nothing on them but the DeCSS code. The Court noted that if a site Corley linked to had the DeCSS code and also a lot of other content, then it may have been acceptable.

The Court addressed 1st Amendment concerns, and found that §101(a)(2) could not be used enforce an injunction against a linking site (like Corley's) absent clear and convincing evidence that the person responsible for the link knows that the relevant material is linked to the site, as well as knows that the material linked to the site is technology that may not lawfully be offered, and create or maintain the link for the purpose of disseminating the technology. [4]

Title II: Online Copyright Infringement Liability Limitation Act

Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers.

The limitations are based on the following four categories of conduct by a service provider:

- Transitory communications
- System caching
- Storage of information on systems or networks at direction of users
- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions [2]

In effect Title II –

- Exempts any OSP or carrier of digital information (including libraries) from copyright liability because of the content of a transmission made by a user of the provider's or carrier's system (e.g., the user of a library computer system)
- Establishes “safe harbors” - a mechanism for a provider to avoid copyright infringement liability due to the storage of infringing information on an OSP's own computer system, or the use of "information location tools" and hyperlinks, if the provider acts "expeditiously to remove or disable access to" infringing material identified in a formal notice by the copyright holder [3]

DMCA Takedown Notice

The DMCA Takedown Notice provides a mechanism for copyright holders to request an Internet Service Provider (ISP), search engine, host or other type of site-owner/manager to remove material that is infringing their copyright. Unlike other aspects of copyright laws, the DMCA Takedown process does not require a person to have a registered copyright. [5]

The DMCA Notice needs to establish-

- The ownership of the copyright
- That the alleged infringement is *not* covered by an exception such as Fair Use or free speech laws
- That the copyrighted content is capable of online infringement i.e. it is a digital file-
    - Text (TXT, RTF, DOC, DOCx, PDF, PPT, PAGES, etc.)
    - Images, pictures & photos (BMP, EPS, SVG, JPG, JPEG, GIF, PNG, PSD, RAW, TIFF, etc.)
    - Video (MPG, AVI, RM, MOV, Quicktime, Windows Media Player, RealPlayer)
    - Music & audio (AIF, AU, MP3, MP4, MID, WAV, etc.)

To be effective, a "notice" must be a written communication to a service provider's designated agent that includes "substantially" the following:

- a physical or electronic signature of a person authorized to act on behalf of the owner;
- identification of the copyrighted work alleged to be infringed;
- identification of the material claimed to be infringing or which is the subject of infringing activity;
- information sufficient to allow the ISP's designated agent to contact the complaining party, e.g., address, telephone number, and e-mail address;
- a statement that the complaining party has a good faith belief that use of the material is unauthorized; and
- a statement that the information in the notice is accurate and, under penalty of perjury, that the complaining party is authorized to act on behalf of the owner. (17 U.S.C. § 512 [c][3][A].) [8]

Legal Proceedings from Application of DMCA TITLE II

Case 1: Safe Harbor denied: *A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001)* [6]

The Court of Appeals for the Ninth Circuit held that a peer-to-peer file sharing service could indeed be held liable for contributory and vicarious infringement of copyright. This landmark intellectual property case put an end to any speculation that such services could facilitate copyright infringement, but still shield themselves from any liability due to the fact that it was the users that chose to share illegal copies of protected works.

Napster was an early peer-to-peer file sharing network which could be used for transmitting various files, but which attained massive popularity as a way to share music through .mp3s. Unsurprisingly, major record companies took issue with large-scale distribution of their music

for free, and sued Napster for direct, contributory, and vicarious infringement of copyright in order to protect their intellectual property.

As stated above, the Court ruled against Napster.

The first issue the court dealt with was "fair use." Fair use is a defense to infringement codified at 17 U.S.C. § 107, which states that otherwise infringing activities are permitted if pursued, "[F]or purposes such as criticism, comment, news reporting, teaching … scholarship, or research." In order to determine whether the defense is met in a particular case, the statute directs Courts to consider the following four factors:

- The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- The nature of the copyrighted work;
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
- The effect of the use upon the potential market for or value of the copyrighted work.

In Napster's case, their platform allowed for "repeated and exploitative" copying, which met the meaning of the first factor, even though no sales were taking place. In addition, songs were found to be "close to the core" of the types of creative works intended to be protected by copyright, and entire songs were downloaded, setting the second and third factors against Napster. Finally, the effect of the downloads was found to harm possible album sales, which was the final nail in the coffin of Napster's argument in favor of a fair use defense.

As for the contributory infringement claim, Napster knew of widespread infringement taking place on its system, and its policing efforts were quite thin. Moreover, Napster materially contributed to the infringement, making success on this claim likely for the appellants. Similarly,

the court found that Napster's lack of effort to reduce infringement, combined with the fact that the company financially benefited therefrom, made success on the vicarious infringement claim likely as well.

As a result, the court ordered the creation of an appropriate injunction consistent with its opinion against any of Napster's future infringing activities.

Case 2: Safe Harbor Allowed: *Hendrickson v. eBay, Inc.* [7]

In this case, the Internet auction service eBay was allegedly offering for sale pirated DVD copies of a documentary about the life of Charles Manson called "Manson." Prior to filing suit, plaintiff Robert Hendrickson sent a letter to eBay demanding that the auction site cease and desist "from any and all further conduct considered an infringement(s) of [plaintiff's] right." eBay responded promptly to this letter, informing Hendrickson of its termination policy for repeat infringers and requesting that the plaintiff submit proper notice under the DMCA by providing more detailed information regarding the alleged infringing items, including identifying the specific eBay item numbers corresponding to the copies of "Manson" for sale. The plaintiff refused to provide this information and proceeded to file copyright infringement suits against eBay.

At trial, Hendrickson did "not dispute that he ha[d] not strictly complied with Section 512(c)(3)." The U.S. district court instead considered whether the plaintiff's imperfect notice satisfied the DMCA's "substantial" compliance requirement. The court noted that Hendrickson did not include in his notice a written statement attesting to the good faith and accuracy of his infringement claim, as required by § 512. In addition, the plaintiff failed to provide eBay with sufficient information to allow the service provider to identify the auction listings that allegedly offered pirated copies of "Manson" for sale. This failure further rendered Hendrickson's notice improper under the DMCA. Therefore, the court ruled, eBay was under no

obligation to remove the allegedly infringing material on its system. The court went on to consider eBay's eligibility for safe harbor under § 512(c) and determined that it satisfied all the statutory conditions. The DMCA thus having shielded eBay from liability, the court granted eBay summary judgment on the copyright infringement claim.

Safeguards to comply with the DMCA: A ISP's Perspective

Educational institutions are prominent Internet Service Providers, and the following DMCA safeguards have been compiled by referring the websites of Educause [8] and a few higher education institutions.

1. **Register** the institution's Digital Millennium Copyright Act (DMCA) Designated Agent with the U.S. Copyright Office.

   Link: http://www.copyright.gov/onlinesp/agent.pdf

   Registering an Agent with the Copyright Office is necessary for the institution to avail itself of the DMCA's safe harbor under 17 U.S.C. Section 512(c), which protects the institution, as an Internet Service Provider (ISP), from liability for copyright infringement occurring on your network at the direction of users.

2. Have institution **policies and procedures** in place for handling DMCA takedown notices.

   The University of Denver follows these steps- [9]

   First and Second Complaints

   When practical, Network Security will notify the person responsible for the possible infringement at his or her @du.edu e-mail address and ask that the person either stop distributing the contested material or submit a counter notification.

   When it is impractical to notify the person responsible via e-mail or when a reasonable time has passed without a receiving a satisfactory reply to an e-mail notification, Network

Security will block Internet access to the contested material. The blocking method may vary from case to case. Some commonly employed methods are listed below. Other blocking methods may also be used. If the material resides on a server managed by the University of Denver, the material may be moved to an inaccessible location or removed from the server. If the material resides on a device not managed by the University of Denver, Internet access to that device may be blocked. If the material resides on a device that must be "logged on" in order to connect to the University of Denver network, "log on" privileges for the person responsible may be suspended. The complaint will be considered resolved when the person responsible for the possible infringement notifies Network Security that distribution of the contested material has stopped or a counter notification has been approved.

Subsequent Complaints

Network Security will block Internet access to the contested material. If the person responsible is a student, the case history will be forwarded to the Office of Citizenship and Community Standards. Internet blocks will remain in effect until the Office of Citizenship and Community Standards informs Network Security that the matter has been resolved and Internet access can be restored. If the person responsible is an employee, the case history will be forwarded to the employee's supervisor, the employee's division supervisor or another office appropriate for dealing with complaints about the employee's behavior. Internet blocks will remain in effect until that office informs Network Security that the matter has been resolved and Internet access can be restored.

3. Have **Technical safeguards** in place –The University of Denver uses an Anagran device to help manage bandwidth utilization on campus. [9]. A university may also have advanced firewalls to block ports which engage in peer-to-peer file transfers.
4. The institution should be aware of (in policy and in practice) the Situational Requirements for **Safe Harbor**:
    - It cannot **post** the infringing content itself.
    - It cannot know that the content infringes a copyright, or be **aware** of facts that would make it obvious that the content infringes a copyright.
    - It cannot receive any **financial benefit** that is directly tied to the infringing content.
5. Post a DMCA Notice on the institution's website. It is recommended that the institution works with an attorney on getting one drafted.
6. **Comply** fully and promptly with any DMCA Takedown Notices you receive from anyone claiming a copyright infringement on your website. Steps for compliance include: [10]
    - **Remove or disable** the allegedly infringing material as quickly as possible.
    - **Notify** the source of the allegedly infringing material (usually the listing agent) of the claim of infringement in case they want to file a counter-notice – i.e., a denial that the material is infringing anyone's copyright.
    - If a **counter-notice** is provided, this must be passed on to the alleged copyright holder.
    - If the alleged copyright holder does not file suit within 10 days after being provided a proper counter-notice, the material can be restored.

7. The institution can also have mandatory **Educational and Awareness programs** which address about file-sharing, DMCA, and copyright infringements.
8. Outsourcing IT Infrastructure – The institution can mitigate the risk. According to the Educause website, “anecdotally, institutions that have outsourced their IT infrastructure, particularly in the residence halls, have found that they no longer receive DMCA notices.”

References

1. History and Overview of the DMCA - FindLaw. (n.d.). Retrieved from http://smallbusiness.findlaw.com/intellectual-property/history-and-overview-of-the-dmca.html
2. Digital Millennium Copyright Act of 1998. (n.d.). Encyclopedia of the First Amendment. doi:10.4135/9781604265774.n427 https://www.copyright.gov/legislation/dmca.pdf
3. DMCA: The Digital Millennium Copyright Act. (2012, September 05). Retrieved from http://www.ala.org/advocacy/copyright/dmca
4. Universal City Studios, Inc. v. Reimerdes. (n.d.). Retrieved from http://www.invispress.com/law/copyright/reimerdes.html
5. Hawkins S. (2015, December 08). How To File A DMCA Takedown Notice. Retrieved from http://sarafhawkins.com/how-to-file-dmca-takedown/
6. Case Study: A&M Records, Inc. v. Napster, Inc. (2013, August 01). Retrieved from https://onlinelaw.wustl.edu/blog/case-study-am-records-inc-v-napster-inc/
7. Digital Millennium Copyright Act of 1998. (n.d.). Encyclopedia of the First Amendment. doi:10.4135/9781604265774.n427 http://www.ipmall.info/sites/default/files/hosted_resources/crs/RL32037_051104.pdf
8. DMCA FAQ. (n.d.). Retrieved from http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/educause-policy/issues-and-positions/intellectual-property/dmca-faq
9. Software Copyright Infringement and Litigation. (n.d.). Judiciary-Friendly Forensics of Software Copyright Infringement, 35-55. doi:10.4018/978-1-4666-5804-2.ch002

http://www.realtor.org/sites/default/files/handouts-and-brochures/2014/window-to-the-law-website-copyright.pdf

10. Digital Millennium Copyright Act. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act