DIGITAL RIGHTS MANAGEMENT

Dr Varsha Updhaya

Vivek Wilson

Digital rights management is a technology that creates certain conditions about how some digital products can be used and shared. It was set up as a system for the protection of digital works. Then, Digital Rights Management (DRM) is a system created or designed to protect the unauthorized duplication and the illegal distribution of copyrighted product. Once the internet becoming widely used, it was easy for pirates to copy and illegally sell a variety of marketed digital information and products. Therefore, this type of technology and system prevents users from doing things with content that the content providers do not wish them to do.

Digital Rights Management, also sometimes called ECMS, or electronic copyright management systems, are technologies designed to automatically manage rights in relation to information. This can include preventing copyright works and other information from being accessed or copied without authorization and establishing and enforcing license terms with individuals. DRM is a form of continual protection that protects works and manages rights at all times, no matter where the works are located or who has the possession of them. DRM attempts to promote authorized use of a copyright work, in part by precluding the possibility of copyright infringement. DRM systems comprise a number of technological components, which can include encryption, a surveillance mechanism, database of works, owners and users, license management functionality and Technological Protection Measures (TPMs).

4.1 ACCESS AND COPY CONTROLS

The simplest way to pursue copyright goal of ensuring that only the users who pay for a work get to enjoy a digital copy of it, is to write software that tries to limit reproduction. Generally speaking, such software falls into two categories access controls and copy controls.

Access controls are a category of architecture that is designed to prevent a user from getting a first copy of a work unless they have a license to do so. Copy controls are snippets of software that try to stop audience members from making a reproduction of work once they have obtained a copy.

Access controls, for what they are worth, are comparatively easy to implement. A website that requires customers to pay a fee before being offered a download is a perfect example. True access controls can also be implemented in physical media by using a broadcast encryption schemes. No payment, no key, no access. One philosophy on the matter is that there is little point in trying to make access controls robust if practical users will just share the works they have legitimately purchased access to[1]. In order for perfect access controls to deliver much more power to copyright holders, they need to be accompanied by strong copy controls. Unlike access controls, true copy controls are impossible to implement on general purpose computers. Ordinary computers are capable of replicating any information they have access to.

Instead, those who want to design copy controls without assistance from hardware are reduced to designing copy inhibitors instead. Copy inhibition techniques resemble access controls but with some conceptual differences. The DVD CSS scheme, for instance, was predicated on the idea that under controlled software would never get access to the work. It would only be displayed by certain "authorized" restricted pla waayer software--- so the user

1 This is most especially true if there is some widely used distribution system---- like a P2P network---that means that one single sharing user can give a copy to any other user who wants to a pirated copy.

could see a film on their screen or TV but would never obtain a digital copy. No first copy, no later copy. Of course, the "authorized" restricted player software can always be edited into unrestricted player software.

4.2 TECHNOLOGICAL PROTECTION MEASURES

While ex post legal action provides one remedy for copyright infringement or any other illegal act, it is not a complete solution. Legal action is expensive and civil actions against impecunious plaintiffs are usually a waste of time. A far more seductive solution for right holders is to prevent, by some technological means, the unwanted copying in the first place. A lesser adjunct would be to embed some form of identifying information in the material which would be to embed some form of identifying information in the material which would establish that a person had exceeded the copying permission.

If an effective technological protection regime could be implemented (this is expressly contemplated by the WCT), then legal protections would almost become moot. Record companies could distribute their music electronically without worrying about widespread piracy; movie studios could do likewise.

Indeed, some believe that copyright is not under threat but is instead at its apogee. With the advent of technologies such as trusted systems, it can be argued that copyright has been perfected.

4.3 ENCRYPTION SCHEMES

An important component of secure delivery of digital data is the use of encryption schemes to remove the ability to access the data without authorization.

Public key cryptography refers to cryptographic system requiring two separate keys one to lock or to encrypt plain text, and one to unlock or decrypt the cyber text. Neither key will do both function. One of these keys is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from

the public key to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Although in this latter case, since encrypting the entire message is relatively expensive computationally, in practice just a hash of the message is encrypted for signature verification purposes.

4.4 DeCSS

The discussion of Napster[2] may have suggested that the music industry was the only intellectual property industry which was under threat. Not so. With the unleashing of DeCSS, the motion picture industry also got very scared very quickly. The motion picture industry supported the widespread use and development of Digital Video Discs (DVDs). A DVD holds more than a CD; an entire movie and extra bonus features can be coded on a single disc. The video and audio could also be digitally enhanced: appealing for people with home cinemas.

4.4.1 THE LITIGATION

The motion picture industry sued in the United States District Court for the Souther District of New York, claiming that DeCSS was a "circumvention device" within the meaning of DMCA. The plaintiff did not sue the manufacturers of DeCSS(who were unknown) but people who hosted the DeCSS code on Web sites or linked to it. The court agreed with the plaintiff's arguments[3], and issued an injunction restraining the parties to the case from distributing DeCSS[4].

2 A&M Records, Inc v Napster, Inc, 239 F. 3d 1004 (2001)

3 *Universal* City Studios, Inc v. Reimerdes, 111 f. Supp. 2d 294 (S.D.N.Y. 2000)

4 *Id*

Effective control of access Judge Kaplam first found that although CSS was not a strong cipher, it nonetheless effectively controlled access to DVDs within the meaning of DMCA[5]. As the only purpose of DeCSS was to circumvent CSS, in was a prima facie violation of the circumvention provisions of the DMCA[6].

4.4.2 DMCA DEFENSES

The defendant's primary defense was that the DeCSS was not written to enable the piracy of DVD movies but to further the development of a DVD player under the Linux operating system[7]. However, contentions based on this argument failed. Primarily, this was because the defendants were trafficking in the circumvention device, not creating it. The traffickers did not do any reverse engineering, therefore could not avail themselves of the reverse engineering for inter operability exception[8]. Even if they did author them, it could not be contended that the sole purpose of DeCSS was to enable a Linux DVD player to be created: DeCSS was developed and ran under Windows and, additionally, the development of DeCSS was held to be "an end in itself[9]". The existence of these subsidiary motivations vitiated the theoretical availability of the defense.

5 *Id* at 317-18

6 *Ibid* at 318-19

7 Id at 319

8 Id at 320

9 Id

Additionally any public disclosure of the information nullifies the availability of the defense[10]. Likewise, none of the defendants were engaged in bona fide encryption research or security testing and could therefore not avail themselves of those exceptions[11].

4.5 ANTI-CIRCUMVENTION LAWS

The case with which copy protection systems were broken motivated a complicated global legislative response: the development of anti-circumvention laws. With variations in detail, these laws prohibit the creation, use, and distribution of devices (or services) that extract works from the control of DRM systems. The process of including those rules in the world's copyright statutes began in earnest with the so called Lehman "white paper" (Information Infrastructure Task Force 1995) and is ongoing. The most significant steps were the agreement on the WIPO Copyright Treaty in 1996, the passage of the U.S Digital Millennium Copyright Act in 1998, and the adoption of the EU Copyright Directive in 2001. Australia implemented anti-circumvention laws (and the other requirements of WCT) with the Digital Agendas Act in 2000 but was forced to adjust them with the US-Australia Free Trade Agreement in 2004. Similar harmonization to the DMCA has been required of other nations entering bilateral trade agreements with the United States. As of this writing, a handful of developed countries are still navigating the turbulent politics of WCT implementation (the most prominent being Canada and Spain).

Anti-circumvention laws have proved extremely unpopular with the technical communities that are regulated by them. In logical terms, there is no clear distinction between the discussion of cryptography and the creation of tools to break it. Technical minds have tended to interpret this fact as making it impossible or absurd to prohibit one without prohibiting the other. But while arguments from freedom of speech had earlier persuaded the U.S courts that

10 *Id*

11 Id at 321

restrictions on the export of cryptography software violated the first amendment[12], they were ineffective in defending hackers who distributed tools for circumvention DVD copy protection.[13] Anti-circumvention laws have also been criticized for their possible effect in relation to hopelessly technical protection measures for threatening to eliminate user rights such as fair use in the United States[14], and for excluding the users of free/open source software from legal access to cultural works. However fairly based these restrictions are, they do not directly interfere with the law's operation. With only a few hiccups, anti-circumvention rules appear to be achieving one of their proponents highest priorities: the elimination of commercially purchasable means to opt out of whatever restrictions a copyright industry might decide to impose[15]. They have been much less effective at preventing the development and distribution of circumvention devices in general. Especially where DRM can be neutralized with software alone, that software has spread rapidly regardless of the law[16]. Preventing diffusion of that sort is fair harder than preventing P2P file sharing, because the volumes of data involved are far smaller.

12 See Bernstein v US Dept. of Justice, case documents archived at http://www.eff.org/privacy/Crypto_export/Bernstein_case

13 See Universal v Reimeredes, case documents archived at http://www.eff.org/IP/Video/MPAA_DVD_cases

14 17 U.S.C 1201, and especially the 'tracking' causes of action in 17 U.S,C. 1201 a 2 A, effectively eliminate these rights, because users cannot obtain the tools necessary to enjoy them.

15 This victory has been decisive in the United States, although there have been a few derivations elsewhere. Australia is one example----- See Stevens v Kabushiki Kaisha Sony Computer Entertainment [2005] HCA 58; the ruling is partly an artifact of the particular architecture of the access controls on the play station(see paragraphs 130-144), but it has been sufficient to ensure that Australian consumers can purchase PlayStations and DVD players that are free from DRM and region coding restrictions. A Finnish ruled that the CSS encryption used on DVDs did not constitute an "effective" technical protection measure; see Helsinki District Court case R 07/1004, 25 May 2007, http://www.turre.com/css_helsinki_district_court.pdf.

16 This can be seen by the ease with which searches of many types yield up copies of libdvdcss, PlayFair, QTFairuse, FairUse4WM, and other widely illegal circumvention software.

4.6 ANTI-CIRCUMVENTION LAWS TO PROTECT DIGITAL RIGHTS: AN INDIAN PERSPECTIVE

Though the digital media provides commercial advantages to the copyright owner, those advantages could be a nullity because easy reproduction and distribution of digital works increases piracy and to track the proliferation of copyrighted works. In order to prevent piracy and to track the proliferation of the copyrighted works, Digital Rights Management (DRM) systems such as encryption, watermarking, fingerprinting and so on have evolved. Rather than tracking illegal uses after they occur, the latest DRM technologies seek to prevent illegal uses at the first place. New technologies like the Windows Media Rights Manager (WMRM) have great amenities to protect digital content. WMRM protects digital audio and video content not only until files are transferred to the user but also even after they are transferred. Microsoft's Palladium is an example of how strong DRM technologies would be in the near future.

Though DRM systems are getting stronger by the day, someone would definitely find a way to break them and that would result in free distribution of the content without the copyright owner's authority. In order to prevent braking/circumvention of the DRM systems the support of law is very essential. To meet this need, laws have been enacted in various nations prohibiting circumvention of DRM systems designed to protect the digital rights of the copyright owner. Such laws protect the rights by making circumvention of technology measures to protect digital content illegal.

Anti-circumvention laws provide strong protection to the copyright owners that they deprive the public of the rights they have over the copyrighted works. As circumvention would be illegal, any such measures to make fair use of the work, would also be illegal, thus depriving public of their rights to free use. Therefore the anti-circumvention laws give rise to a conflict in this modern era which springs bad consequences. The world is today struggling to find an

amicable solution to this problem. Under such circumstances this article explores the need for an anti-circumvention law in India and other developing countries.

4.6.1 INDIA AND ANTI-CIRCUMVENTION LAWS

India doesn't have any anti-circumvention laws to protect DRM technologies; the Indian legislature hasn't implemented the WCT and WPPT. India is a country filled with piracy, as the copyright law is not strictly enforced. Not many authors in India really bother about registering their works with the copyright office or enforcing their copyrights. Enough importance is not being given to copyright and other forms of intellectual property in India due to complicated reasons.

Though the existence of widespread piracy is fatal to the ends of copyright law, it has certain advantages considering the fact that the copyrighted content is out of reach of the people of India because of the economics involved. The availability of pirated copies provides advantages to both content owners and users.