Digital Balance

Au, Tin Lun (Bruce)

May 16, 2002

Massachusetts Institute of Technology

Harvard Law School

Spring Semester, 2002

MIT 6.805/6.806/STS085: Ethics and Law on the Electronic Frontier

Advisors

Joe Pato

Hal Abelson

Table of Contents

Table of Figures

Acknowledgements

I would like to thank my advisors Joe Pato and Hal Abelson for their guidance. I would also like to thank Butler Lampson, Mike Godwin, Jonathan Zittrain, Tim Gorton and Jane Jung for their generous input.

Abstract

This paper predicts that the widespread use of digital rights management systems in the future will empower copyright owners to refuse delivering digital content to their subscribers if some software that are in operations on their subscribers' computing environments are unknown to them. Therefore, digital content providers will not leave room for non-infringing uses of their copyrighted work and effectively expand the scope of their exclusive rights beyond the boundary set forth in the Copyright Law. I propose that the Copyright Office should establish itself as a Certificate Authority (CA) and certify software applications it deems compliant with the Copyright Law. Some content providers will choose to honor the Copyright Office's digital certificates, or as I will term "Digital Balance (DB) Certificates," in order to attract subscribers, and deliver content to their subscribers' computers in the presence of the certified software. Since the DB Certificate is voluntary, the content providers retain their right to charge the Copyright Office's decision in courts. The office's certification is not a legal judgment; instead it opens room for the non-infringing uses opportunities of copyrighted work.

Thesis Statement

The U.S. Copyright Office should establish itself as a Certificate Authority (CA) and issue Digital Balance (DB) Certificates to software applications or systems it deems compliant with the U.S. Copyright Law. The market force should compel the content providers to honor the DB Certificates. As a result, the delicate balance between the copyright owners' exclusive right to their work and the promotion of arts and science in the public domain would be restored.

Introduction

Section 8 of Article I of the U.S. Constitution empowers Congress "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." The intent of the Copyright Law is to maintain the delicate balance between the authors' exclusive right to their work and the progress of science and arts in the public domain. This paper presents a solution to restore this balance. In the past, the development of a decentralized file-sharing system in the Internet made it very hard for authors to protect their exclusive rights of their digital content, but the imminent introduction of the digital right management system will change the landscape drastically and enable the authors to expand the scope of their exclusive rights beyond the limit defined under 17 USC 1. I propose that the Copyright Office should issue Digital Balance (DB) Certificates to re-open the door for non-infringing uses of digital copyrighted work. See Figure 1 for a pictorial representation of the idea presented above.

In this paper, I propose a solution to this future problem. Part I states the future that I foresee and its potential problem. Part II outlines the administrative and technical implementations of my proposed solution, namely the establishment of the U.S. Copyright Office as a Certificate Authority that certifies software applications or systems which it considers compliant with the U.S. Copyright Law. Part III evaluates, and demonstrates the viability and effectiveness of the proposed system by arguing that the law, the architecture, the market and the norm are mostly in favor of the proposed solution. It addresses some concerns of various stakeholders: the copyright owners, the

hardware and software industry, the government and the consumers. Part IV discusses the weaknesses of the system and compares the proposed solution with some alternative designs. Part V explains the reasons why the future problem that I foresee in Part I is probable.

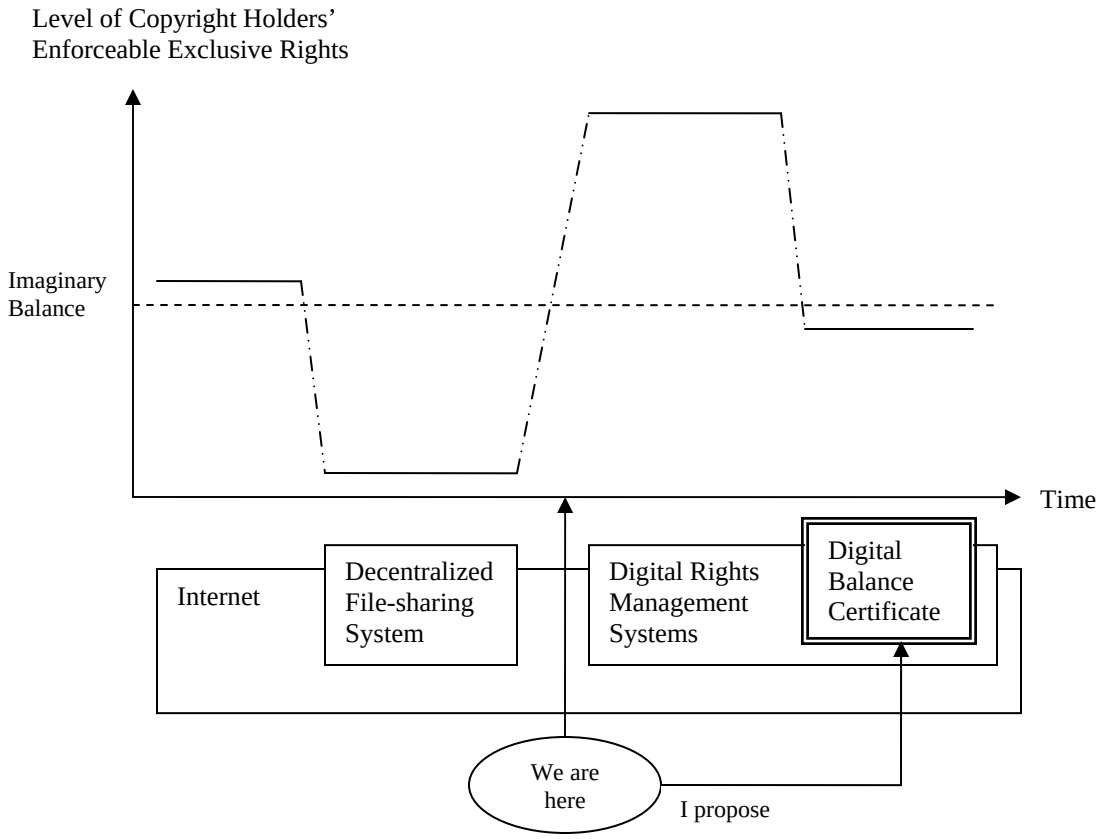

Figure 1: High-level Overview. The Imaginary Balance is the balance between the authors' exclusive right to their work and the progress of science and arts in the public domain

I. The Future and its Problem

Digital content providers will have the technical means as well as legal support to preclude any functions other than those they determine, from being performed on their digital contents. In practical terms, their subscribers will not receive any copyrighted materials from content providers if their computing environments contain software applications that are not certified by the providers. Software applications have to authenticate themselves to a digital rights management system before being loaded to the computing environment. Since this is so, the digital rights management system is able to

report the status of the computing environment to the content providers and let them decide whether copyrighted work should be delivered. (I will discuss why the content providers' will acquire such technical means and legal support to prevent any non-infringing uses of their work through decentralized file-sharing systems in Part V.) Therefore, copyright owners will have the power to effectively expand the scope of their exclusive rights beyond the limitations defined under 17 USC 1, because they can among other things, effectively eliminate any possibilities for fair use of their copyrighted work for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, defined under 17 USC 107.

If we put Sony Corporation of America v. Universal City Studios, the definitive Supreme Court case regarding copyright into this future, Universal City Studios would be able to detect whether Sony's video tape recorders, Betamax is hooked up to their subscribers' TV's or not, before deciding whether they still want to deliver them the TV programming. Hence, the Sony v. Universal Studios case would not have existed. The creation of Digital Balance (DB) Certificates proposed in this paper is to prevent content providers from having too much control over their copyrighted work.

II. The Solution

II.1 Overview

The U.S. Copyright Office would issue digital certificates called Digital Balance (DB) to software applications that it considers compliant with the Copyright Law. It signed the DB Certificates with its private key. Some content providers would decide to honor the DB Certificates and deliver their copyrighted materials to their subscribers' computers in the presence of DB certified software applications. The process of securely authenticating the DB certified programs by the content providers will be discussed in Part III.2.

In order to obtain a DB Certificate from the Copyright Office, a software developer would have to submit its software functions description and technical specifications to the Copyright Office for examination with an application fee. A Digital

Balance Division within the Copyright Office would be responsible for evaluating the documents based on the Copyright Law and related Supreme Court cases such as Sony v. Universal City Studios. After the Copyright Office concludes that the software program or system does not allow infringing uses of copyrighted content, it would issue the software developer a preliminary DB Certificate that includes items such as the certificate's ID, date of publication and name of the application, the version of the application, the date of expiration and a list of functionalities provided by the software application. The software developer would employ a third party to test the software and produce a quality control report that evaluates the adherence of the actual software to its specifications within on average 9 months after the software is released. The Copyright Office would decide whether a software application's DB Certificate should be renewed based on the quality control report and the actual program. The Copyright Office can reject the applications by issuing a rejection at any point in the course of the application process. Figure 2 summarizes a successful DB Certificate application process. Again, the execution environment that supports this system will be described in Part III.2.

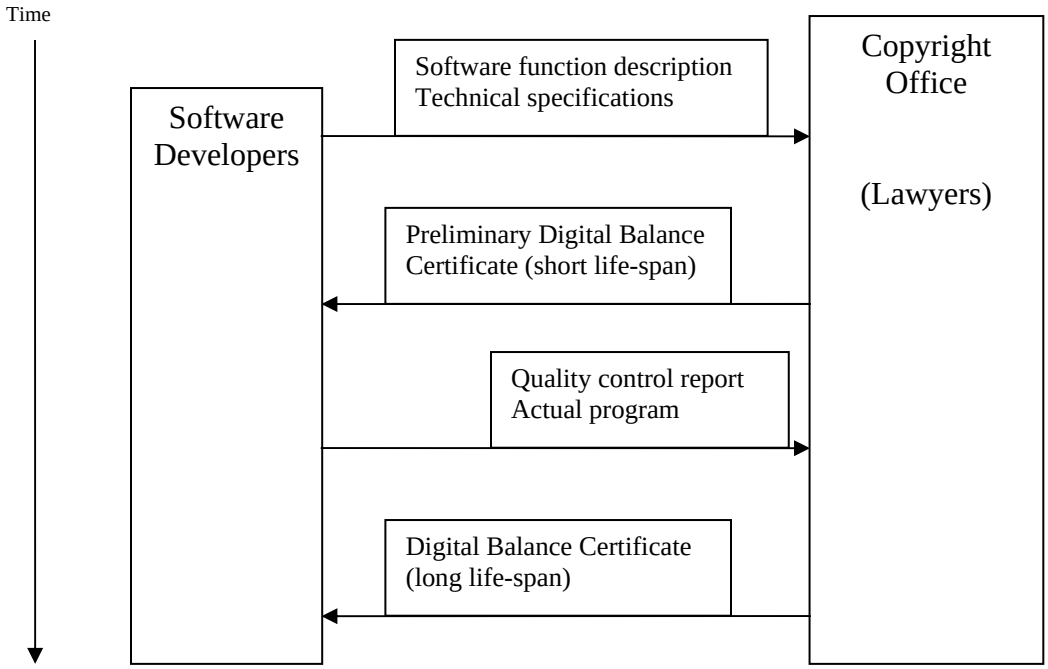

Figure 2: This is an example of a successful application of the Digital Balance Certificate. The Copyright Office can reject the applications by issuing a rejection at any point in the course of the application process.

Some content providers may honor the DB Certificates and deliver their digital contents to their subscribers while DB certified software applications are present on subscribers' computing environments. Some may not. Naturally, content providers would retain their rights to challenge the DB software applications in courts when for example; they deem the software developers liable for contributory and vicarious copyright infringement.

II.2 System Administration

The Copyright Office would create a new division to entertain all of the applications. With the division, the panel that has the authority to approve the software applications would be predominately composed of copyright lawyers, and includes representatives from the content providers, software companies and consumer groups. The division also would have staff for administration and technical maintenance. This section explains in detail the decision-making process and the criteria of the certification.

II.2a Decision-making Process

The software developers, hereafter referred to as applicants would have to identify themselves and submit two documents – the software function description and technical specifications – in order to apply for the Digital Balance Certificates. The software function description exhausts the list of functions that can be performed by the software and gives arguments on why the applicant's software does not constitute copyright infringement. The technical specifications would be stored in the Copyright Office for future reference when the applicant submits its quality control report.

With this information in hand, the panel would attempt to mimic the courts' rulings as much as possible when they are evaluating the legitimacy of the software. Although content providers would be likely to charge software developers for contributory and/or vicarious copyright infringement, instead of direct infringement, the copyright owners have to prove, among other things, that there has been a direct

infringement by someone[1]. Therefore, the primary question the panel has to ask before they would issue a preliminary Digital Balance Certificate to an applicant is whether the use of copyrighted work enabled by the software application constitute direct copyright infringement or not. They would do so by referring primarily to the Copyright Law, especially 17 USC 107 – fair use and the precedence set by previous Supreme Court cases. The criteria of certification will be discussed in the next section. There are two reasons for issuing a preliminary DB Certificate. First, it would enable applicants to develop their new software with higher confidence of them being certified. Second, it would allow applicants to release their software without significant delay so that they can be responsive to the market as much as possible. This reduces the amount of otherwise unbearable overhead on the applicants' part.

In order to receive a DB Certificate of longer long-span, applicants would have to employ a third party that has no conflict with interest in the subject to create a quality control report. The report would evaluate the accuracy of the software function specifications in describing the actual functioning of the program as well as the discrepancy between the functions stated in the specifications and the functions that can be performed by the actual program. Common security evaluation standard such as United Kingdom Information Technology Security Evaluation and Certification Scheme (UK ITSEC) takes 6 months to a year to evaluate a software application. Therefore, the applicants would have just enough time to submit their quality control report in around 9 months after the first date of releases of their software. The panel would then base its final decision on its direct experience in manipulating copyrighted work with the software and the recommendations of the quality control report. The procedure for issuing DB Certificates will be discussed with more detail in Part II.3b.

II.2b Criteria of Certification

This section proposes the criteria of certification that guides the panel's decision. The major criteria are that the functions of the software do not exceed the boundary of

1 See Fred von Lohmann, *IAAL: Peer-to-Peer File Sharing and Copyright Law after Napster,* Berkeley Center for Law & Technology, 2001

fair use defined under 17 USC 107 - limitations on exclusive rights: fair use and 17 USC 1201 – circumvention of copyright protection systems. I will suggest a list of software applications that should successfully be DB certified at the end of the section. However, since non-infringing uses of copyrighted work by definition cannot be pre-determined; my list of software is by no means exhaustive or definitive.

17 USC 107 states that

> "the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright."

The Panel would consider the four factors defined under 17 USC 107 when determining whether the functions enabled by the software applications are non-infringing or not. The four factors are

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (4) the effect of the use upon the potential market for or value of the copyrighted work.
> The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors

17 USC 1201 states that

> (1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.
> (2) 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;
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

The panel would also draw references from relevant Supreme Court cases such as Sony Corporation of America v. Universal City Studios in which, the Supreme Court

decided that the use of Betamax video tape recorders (VTR's) to record some copyrighted works which had been exhibited on commercially sponsored television by the content providers a non-infringing use and therefore judged that Sony was not liable for contributory copyright infringement. Justice Stevens, in the course of his delivery of the Court's opinion gives another guideline that may not be immediately apparent from the four factors mentioned above: the existence of some meaningful likelihood of future harm on the potential market for the copyrighted work is sufficient to challenge a noncommercial use of that copyrighted work.

> "A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work. Actual present harm need not be shown; such a requirement would leave the copyright holder with no defense against predictable damage. Nor is it necessary to show with certainty that future harm will result. What is necessary is a showing by a preponderance of the evidence that some meaningful likelihood of future harm exists. If the intended use is for commercial gain, that likelihood may be presumed. But if it is for a noncommercial purpose, the likelihood must be demonstrated."

This guideline is very relevant to today's situation where the use of Internet is pervasive. One piece of software that enables noncommercial use of a copyrighted work can be widely available to the public and hence be likely to cause future harm on the potential market for the copyrighted work.

The Court also gives another guideline in the event that the content providers can not demonstrate that the use of certain articles of commerce induce future harm on the potential market of their copyrighted work. The guideline for this particular case is that the copyright holders have no power over the distribution of that particular article of commerce if it is capable of commercially significant non-infringing use. Justice Stevens claimed that

> "…the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."

In summary, the panel certifies software applications that it deems safe from direct copyright infringement in order to safeguard room for non-infringing uses of copyrighted work. There would have been a direct infringement by someone to make

software developers liable for contributory and/or vicarious copyright infringement. Therefore, the Copyright Office's certification has no legal power and its sole purpose is to protect content providers' copyrighted work from being abused in the era of Internet. Hence, the content providers can disagree with the Copyright Office and charge any software developers and consumers for indirect copyright infringement and direct infringement respectively in courts.

The following list of imaginary software applications demonstrates some functions that content providers may not allow to be performed on their copyrighted work, but are likely to be considered non-infringing uses by the Copyright Office:.

1. Allows users to record an online TV show or radio broadcast onto their machines;
   prohibits them from forwarding the content over the network but;
   allows them to replay the content on the same machine for an unlimited amount.
2. Allows users to mark, paint and make changes to digital images but;
   disallows them to send the derivative work to elsewhere over the network or print it out.
3. Allows users to make a clip of a digital movie or a digital song;
   allows them to replace the sound track of a digital movie with another song or insert new clips into the movie but;
   disallows them from sending the derivative work to a third party.
4. Allows users to type up notes while reading an expensive company research report in digital form on the screen;
   disallows users from printing or forwarding the report but;
   allows user to print out or foward the notes that are typed up to a third party in that session.

II.3 Technical Infrastructure

This section describes the cryptographic protocol that the applicants and the Copyright Office would use, the procedure of certifying and revoking a software application, the contents of a Digital Balance Certificate and the confidentiality of the system.

II.3a Cryptographic Protocol - SSL

Applicants and the Copyright Office would communicate over the Internet through an improved version 3 of the secure socket layer (SSL) protocol that prevents

two known attacks: version-rollback attack and ChangeCipher attack.[2] The proposed system also requires the applicants to use a 128-bit key size to protect the key against brute force attack. As SSL is already a widely used cryptographic protocol, it has been subject to a significant amount of on-field testing. Therefore, the proposed system chooses SSL for both its popularity and security.

II.3b Certification Procedure and Revocation

A DB Certificate would certify a software application that the Copyright Office deems free from direct copyright infringement. It would include items such as the certificate's ID, date of publication and name of the application, the version of the application, the date of expiration and a list of services, or properties, provided by the application, i.e., content type handled, whether it saves content to disk, etc. The language used to express functionalities of the application must be consistent with the standard adopted by the future digital right management system. The Copyright Office then signs the binary of the DB Certificate with its private key. The Copyright Office changes its asymmetric key pairs annually to enhance security. Figure 3 illustrates the process of certification. The Copyright Office's signed DB Certificate is critical for the software to successfully authenticate itself to a digital right management system. This authentication process will be discussed in more detail in Part III.2.

[2] See Saltzer, J. H., and Kaashoek, M. F., Topics in the Engineering of Computer Systems, MIT 6.033 class notes, draft release, version of January 27, 2002, 6-86 ('Version 3 of SSL accepts connection requests from version 2 of SSL. This opens a version-rollback attack, in which an attacker convinces the server to use version of 2 of the protocol, which has a number of well-documented vulnerabilities, such as the cipher substitution attack. Version 3 appears to be carefully designed to withstand such attacks, but the specification doesn't forbid implementations of version 2 to resume connections that were started with version 3 of the protocol. The security implications of this design are unclear. One curious aspect of version 3 of the SSL protocol is that the MAC in the Finished message does not include the ChangeCipher message. As pointed out by Wagner and Schneier, an active attacker can intercept the ChangeCipher message and delete it, so that the server and client don't update their current cipher suite. Since messages during the handshake are not sealed and authenticated, this can open a serious security hole. Wagner and Schneier describe an attractive attack that exploits this observation. Currently, widely used implementations of SSL 3.0 protect against this attack by accepting a Finished message only after receiving a ChangeCipher message. The best solution, of course, would be to include the ChangeCipher message in the MAC of the Finished message, but that would require a change in the specification of the protocol.')

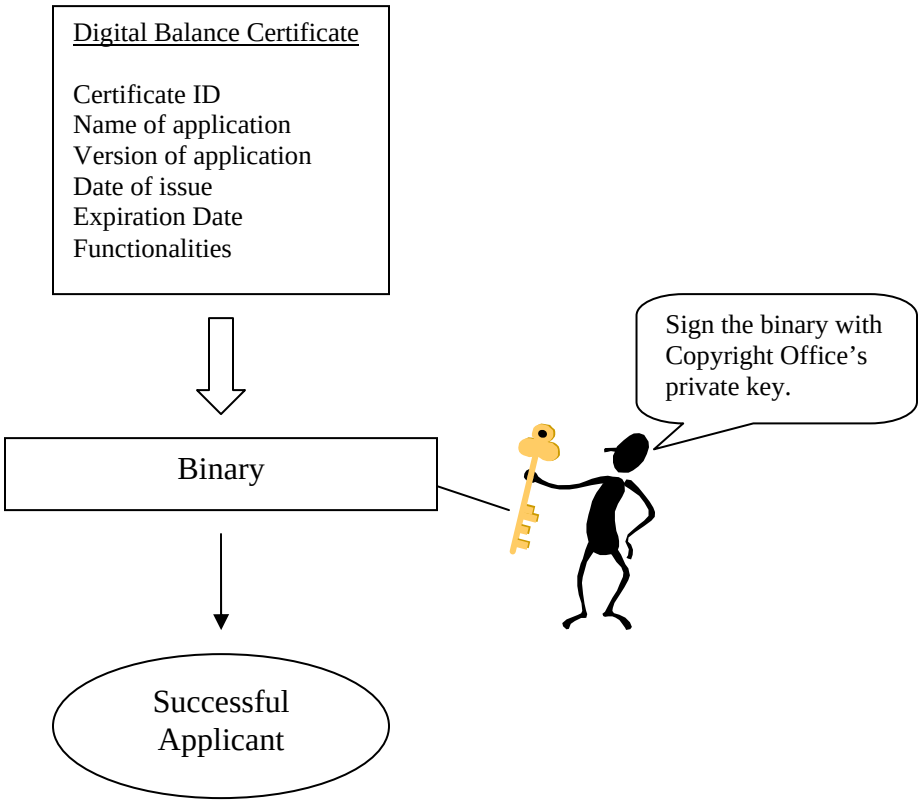

Figure 3: The process of certifying an applicant's software. The Copyright Office sends the signed binary of the DB Certificate to the successful applicant.

The Copyright Office would revoke a certificate by making the certificate's ID public, so that the digital right manage system can disregard it by adding the ID to their own certificate revocation list. The DB Certificates also have expiration dates, so they are automatically revoked when they expire. The Copyright Office would normally set the expiration date to be one year from the date of issue, but it may employ a more complicated scheme to enhance the system's efficiency. For instance, the Copyright Office could set a longer expiration period for software that applies for renewal and set a shorter expiration period for software whose candidacies are more controversial.

II.3c Confidentiality of the Application Process

An applicant cannot apply for a DB certificate anonymously, but the Copyright Office also can not reveal any of the information submitted by an applicant, the applicant's identity, or the status of his application to any third party except the courts.

The Copyright Office would maintain a record of all the submitted materials in a secure storage for future reference.

III. System Evaluation

This section evaluates, and demonstrates the viability and effectiveness of the proposed solution: establishing the Copyright Office to certify software applications that it considers compliant with the Copyright Law. The copyright owners, the hardware and software industry, the government and the consumers are various stakeholders of the system and they all fall under one of the four main forces that shape a behavior in today's society: law, architecture, market and norm[3].

III.1 Law

This section illustrates why the proposed solution is compliant with the Copyright Law, which it aims at safeguarding. The focus of the analysis is on the proposed solution's compliance with the anti-circumvention provisions and the concept of fair use defined in the Digital Millennium Copyright Act (DMCA). This section also argues that the Copyright Office is responsible for and is capable of executing the proposed solution.

III.1a U.S. Copyright Law

The proposed system is voluntary and does not require any. Copyright holders and content providers have no obligation to recognize the Digital Balance Certificates issued by the Copyright Office. Although I will argue below that content providers are likely to be compelled to recognize the DB Certificates due to the market pressure, the voluntary nature of the system can be considered a weakness and will be discussed in more detail in Part IV. Nevertheless, this voluntary nature frees the system from running afoul of the provisions in the U.S. Copyright Law. DB Certificates do not legitimize the use of copyrighted work performed by software applications. The Copyright Office simply makes a judgment on whether software enables non-infringing or infringing uses of copyrighted work. Content providers, whether they honor the DB Certificates or not,

[3] See Larry Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, Harvard Law Review (Draft, Fall 1999), P. 506-7

continue to have the right to challenge the software developers of the applications under suspicions for violating the Copyright Law in court.

I in my analysis take one step further and assume that Congress has passed an Act that mandates all digital content distributors to participate in the system and honor the DB Certificates. The content distributors still have their right to challenge the software developers in courts. I argue that the Act will still be compliant with the law because the Copyright Office still only allows *the opportunities* for non-infringing uses of copyrighted work. The Copyright Office will become an independent United States government agency that regulates the copyright system regarding digital work, similar to the Federal Communications Commission (FCC) that regulates interstate and foreign communications by wire or radio.[4] If some certified software applications provide functions that constitute copyright infringement or circumvent technological means that protects copyrighted work and the court rules that the software developers violate contributory or vicarious copyright infringement, the copyright holders will still receive legal remedies from them. The copyright holders are also entitled to charge any direct offenders such as consumers. Essentially, this Act does not widen the spectrum of fair use and access control circumvention, but only attempts to restore the balance between the rights of copyright owners and public in the use of copyrighted works by allowing the possibilities of infringing uses.

U.S. Copyright Office

The mission of the Copyright Office is to promote creativity by administering and sustaining an effective national copyright system.[5] If the content providers eliminate all possibilities for non-infringing uses of their copyrighted digital work, the Copyright Office is responsible for reestablishing a balance between the public's interest and the copyright owners' exclusive right in the digital media. In addition, the Copyright Office is publicly funded, so it is ideal to act as an impartial Certificate Authority to issue DB Certificates. The Copyright Office is also capable of executing the proposed system, as it

[4] See Section 1, Communication Act of 1934
[5] See U.S. Copyright Office, *Strategic Plan 2002-2006*, Part 1 – The Mission and Function of the U.S. Copyright Office, February 2002

has positioned itself to make a fundamental transformation in its public services from paper and hard copy-based processing to primarily electronic processing. It also plans to change its processes from traditional manual capabilities to IT-enabled functions.[6] Lastly, as the Copyright Office currently does not advise on possible copyright violations[7], it employs or contracts copyright lawyers to make the decision in the process of issuing DB Certificates.

Non-infringing uses of copyrighted work cannot be pre-determined by definition. The Copyright Office simply allows opportunities for the public, especially software developers, to perform non-infringing uses but does not define them. Therefore, it does not impact any jurisdiction the courts currently enjoy. The Copyright Office screens the software applications primarily because it makes the proposed system more reasonable and credible for content providers to take part in, in light of the widespread use of decentralized file-sharing systems in the Internet. The effect of decentralized file-sharing systems on content providers will be discussed in more detail in Part V.

III.2 Architecture – Hardware and Software Industry

Code is the architecture that shapes the proposed system. This section explains the execution environment for the DB certified programs and also evaluates the security level of the proposed system.

Both hardware and software companies have to be involved in order to create an execution environment that enables the functioning of the proposed system and they have already been striving towards creating such a computing environment. More than 150 hardware and software companies have joined the Trusted Computing Platform Alliance (TCPA) since the spring of 1999[8]. They envision building a solid foundation for improved trust in the PC over time and agree that the specification for the trusted computing PC platform should focus on two areas – ensuring privacy and enhancing

[6] See U.S. Copyright Office, *Strategic Plan 2002-2006*, Part 3 – Copyright Office Strategic Initiatives, February 2002
[7] See U.S. Copyright Office's Web site at http://www.copyright.gov/fls/fairuse.html
[8] See http://www.trustedpc.org/home/home.htm

security.[9] They have created a specification for a Subsystem that enhances access controls on information stored on a trusted platform. Among other things, a Trusted Platform enables an entity to determine the state of the software environment in that platform and to seal data to a particular software environment in that platform.[10]

Moreover, Microsoft Corporation has already obtained a United States patent (6,330,670) for a Digital Rights Management Operating System (DRMOS), which resembles closely to the vision set forth by the TCPA and provides an example of execution environment that supports the proposed system. This is the abstract of the invention:

> "A digital rights management operating system protects rights-managed data, such as downloaded content, from access by untrusted programs while the data is loaded into memory or on a page file as a result of the execution of a trusted application that accesses the memory. To protect the rights-managed data resident in memory, the digital rights management operating system refuses to load an untrusted program into memory while the trusted application is executing or removes the data from memory before loading the untrusted program. If the untrusted program executes at the operating system level, such as a debugger, the digital rights management operating system renounces a trusted identity created for it by the computer processor when the computer was booted. To protect the rights-managed data on the page file, the digital rights management operating system prohibits raw access to the page file, or erases the data from the page file before allowing such access. Alternatively, the digital rights management operating system can encrypt the rights-managed data prior to writing it to the page file. The digital rights management operating system also limits the functions the user can perform on the rights-managed data and the trusted application, and can provide a trusted clock used in place of the standard computer clock."

The DRMOS described in the patent requires certain configurations of the central processing unit (CPU) in a PC[11], but hardware companies are likely to support the changes considering the participation of Intel Corporation, one of the main CPU producers in the TCPA. The DRMOS, among other things, ensures two requirements: first, trusted applications must be identified in some fashion, and, second, the DRMOS must prevent non-trusted applications from gaining access to the content when it is stored, either permanently or temporarily, on the subscriber computer.[12] In one of the invention's embodiment, the DRMOS identifies an application through a certificate. That

---

[9] See the Trusted Computing Platform Alliance (TCPA), *Building a Foundation of Trust for the PC*, January 2000, P.1

[10] See the Trusted Computing Platform Alliance (TCPA), *TCPA Main Specification Version 1.1a*, 2001, P. 2

[11] See Microsoft Corporation, *United States Patent 6,330, 670*, Hardware and Operating Environment

[12] See Microsoft Corporation, *United States Patent 6,330, 670*, System Level Overview

is where DB Certificates come into play and help content providers trust applications. All in all, the technology for an effective digital right management system that mandates software to authenticate themselves using digital certificates already exists.

III.3 Market

The proposed system is a voluntary program where content providers are not forced to participate. Therefore, the market is the major force that compels content providers to give room for non-infringing uses of their digital work. I argue that subscribing digital content online is an untouched and competitive market that will push content distributors to honor Digital Balance Certificates in order to open as well as win the market. This is also a profitable business perceived by content providers.

Digital content providers bear little cost to store, reproduce and distribute their copyrighted work, compared to the traditional physical content providers. For example, as far as online music goes, apart from the cost, research from companies show that the market is lucrative. Webnoize states that over half of U.S. college students are willing to pay $10 or more per month to use Napster, suggesting the college market alone could generate over $400 million per year in revenues for the service.[13] In Europe alone, the online market for music is expected to soar in value from 333 million euros last year to more than 2 billion euros by the end of 2006, according to research from Jupiter MMXI.[14] It is hard to argue that a certain market is profitable, but I can try to show that subscribing digital content online is perceived as profitable by companies. For instance, Secure Digital Music Initiative (SDMI) is a forum for industries to develop a voluntary, open framework for playing, storing, and distributing digital music necessary to enable a new market to emerge.[15] It has 147 participating companies in October, 2000 and the membership fee is $20,000 per year.[16]

[13] See BBC News, Poor outlook for paid-for online music, September 2001, at http://news.bbc.co.uk/hi/english/sci/tech/newsid_1556000/1556097.stm
[14] See BBC News, Online Music Bonanza, April 2001, at http://news.bbc.co.uk/hi/english/business/newsid_1300000/1300489.stm
[15] See Secure Digital Music Initiative at http://www.sdmi.org/who_we_are.htm
[16] See Secure Digital Music Initiative at http://www.sdmi.org/participant_list.htm

What is certain is that online digital content subscription is an untouched market. Apart from online digital music mentioned above, there is an array of digital contents such as movies, expensive documents and images, TV and radio broadcasts that can be distributed in digital format to the Internet population.

Congress passed the Sherman Antitrust Act in 1890 to maintain economic liberty and eliminate restraints on trade and competition. Antitrust Law is a strong protection against a monopoly on the digital content distribution industry. Moreover, in the case of online music, Congressmen have taken initiative to create a fair ground for competition. Rick Boucher and Chris Cannon introduced the Music Online Competition Act in August 2001 that aims at removing obstacles for the Internet music services such as facilitating them to locate and notify all of the publishers of a particular musical composition and allows them to produce multiple copies of a song in different transmission speeds and different media formats.[17] "The Music Online Competition Act will ensure that consumers have Internet access to legal high-quality music, that creators get paid rapidly, and that competition - rather than lawsuits - will drive this marketplace forward," said Jonathan Potter, executive director of Digital Media Association (DiMA).[18]

In summary, providing digital content online is an untouched and large market that is perceived as lucrative by content providers. In order to compete with each other, some content providers will choose to honor the Digital Balance Certificates to boost their reputation.

III.4 Norm – Consumers

There are yet any major educational campaigns that teach the public about the current statute of the Copyright Law, but there are already companies that advocate the Fair Use Right to make copies of digital content for personal use, not mentioning

[17] Statement of Congressman Rick Boucher, Introduction of Music Online Competition Act, August 3, 2001

[18] See DiMA Applauds Legislation that Supports Consumers, Creators and Competition at http://www.digmedia.org/whatsnew/brief.cfm?file=ACF79FE.htm

consumer groups. For example, Gateway Computer bought a one-minute television spot that promotes the message of "Gateway supports your right to enjoy digital music legally". This is the summary of the TV advertisement provided by a Wired News article on April 11th 2002[19]:

> A man slides a CD into his truck's stereo. Music fills the cabin. The camera pulls back, revealing Gateway CEO Ted Waitt sitting next to a cow. As Elwood's cover of "Sundown" starts, Waitt and the cow begin lip-synching the song.
>
> Black-screen messages pop up.
>
> "Like this song?"
>
> "Download it from Gateway.com."
>
> "Burn it to a CD...."
>
> "Or load it on an MP3 Player."

On top of the idea that making copies for personal use is legal, a generation of Internet users grows up with the idea that swapping files online is legal. The average number of simultaneous users of Napster was 1.57 million in February 2001[20]. A National Law Journal study done by DecisionQuest found that 41.5 percent of 1,000 potential jurors believe that copyrighted music should be freely traded for personal use[21]. The public norm is likely to oppose the notion that a digital rights management system should be ale to dictate all possible uses of digital content.

On the far end of the spectrum of interpreting the fair use doctrine, there are various groups that advocate a broader interpretation of “fair use”. The current statute of the doctrine is that fair use is a defense against copyright infringement, but organization like Digitalconsumer.org advocates changing the statute to give consumers the right to

---

[19] See Brad King, *Are Ads a Gateway to Illegal CDs?*, at http://www.wired.com/news/mp3/0,1285,51719,00.html

[20] See Michael Mahoney, *Report: Napster Downloads Fall 87 Percent Since February*, E-Commerce Times, June 6, 2001, at http://www.ecommercetimes.com/perl/story/10298.html

[21] See Dick Kelsey, Jury Pool Survey - Napster's Chances Good, Newsbytes, Oct. 10, 2000, at http://www.newsbytes.com/pubNews/00/156450.html

"fair use". They propose the Consumer Technology Bill of Rights[22], which gives users the right to

1. "time-shift" content that they have legally acquired.
2. "space-shift" content that they have legally acquired.
3. make backup copies of their content.
4. use legally acquired content on the platform of their choice.
5. translate legally acquired content into comparable formats.
6. use technology in order to achieve the rights previously mentioned.

In summary, the public is likely to have a more liberal interpretation of the fair use doctrine than the content providers do, let alone the content providers' financial interest. Therefore, content providers who recognize the Digital Balance Certificates can claim that they support consumers' "right" to perform non-infringing uses of digital content and are likely to gain reputation as well as subscriptions from them.

IV. Weaknesses

IV.1 Overview

The proposed solution to establish the Copyright Office as a Certificate Authority is a voluntary program and does not force content providers to participate. Content providers have no legal obligation to honor the Digital Balance Certificates issued by the Copyright Office, and are able to determine all the possible uses of their copyrighted materials by themselves. Software companies may not find the business of innovating software applications that respect copyright lucrative and may not take part in the proposed system as well. Lastly, the technology that supports the DB Certificates may also be flawed.

IV.2 Content Providers Do Not Participate

I argue in Part III.3 that the untouched and competitive market of online subscription of digital content will compel content providers to leave room for the public to decide what constitute non-infringing uses of their work. However, the music industry today does regard making a mixed CD of favorite music on computers a piracy practice. The Recording Industry Association of America (RIAA) defines, on their Web site one

[22] See http://www.digitalconsumer.org/bill.html

type of piracy recordings as "the unauthorized duplication of only the sound of legitimate recordings, as opposed to all the packaging, i.e. the original art, label, title, sequencing, combination of titles etc. This includes mixed tapes and compilation CDs featuring one or more artists." Therefore, there are reasons to believe that other digital content providers may follow the music industry's strong stance on interpreting the fair use doctrine and disregard the Digital Balance Certificates. Nevertheless, one can counter-argue that the content providers would learn a lesson from the Sony Corporation of America v. Universal City Studios case, as movie companies receive substantial revenue from movie video today. Unknown fair usage of copyrighted work has the potential to benefit copyright owners.

The proposed solution is essentially an attempt to restore the balance between providing copyright holders' incentives to create and promoting arts and science in the public domain with as little intervention as possible. If the content providers choose other

means to gain market share, rather than allowing room for the opportunities of non-infringing uses of their digital work by recognizing Digital Balance Certificates, the proposed solution will fail. However, the proposed system will at least put the government in a better position for introducing stricter regulations if necessary while introducing new regulation on the market is usually a political nonstarter. Dan L. Burk and Julie E. Cohen presented thorough analysis on the legality of introducing stricter regulation such as mandating content providers to recognize Digital Balance Certificates in *Fair Use Infrastructure for Rights Management Systems*[23].

IV.3 Software Companies Do Not Participate

In order to make the proposed solution successful, software companies must innovate new types of software that respect copyright. One may argue that the overhead of applying for Digital Balance Certificates will hinder the growth of this business. However, the introduction of Digital Balance Certificates also creates a new business

[23] See Dan L. Burk and Julie E. Cohen, *Fair Use Infrastructure for Right Management Systems,* Harvard Journal of Law & Technology, Harvard Law School, fall 2001.

model for software development, despite the fact that the application process certainly takes time and effort from the developers' part. A software company can choose to work for content providers and develop software that complies with content providers' specifications, but the introduction of DB Certificates opens room for them to innovate new applications that were never conceived before. Video tape recorder is a commonplace nowadays but it was a stunning invention at the time it was first introduced. Moreover, the issuing of preliminary DB Certificates to software developers who have only submitted their software function description and technical specifications speeds up the application process in an attempt to allow software developers to release their products to the market on time. In addition, educational institutes can also be another driving force behind the development of the next generation of software that respects copyright.

IV.4 Technology Is Not Yet Ready

The proposed solution also makes the assumption that a certain computing environment, as described in Part III.3, will be in place to support the Digital Balance Certificates. If the technology for building such a computing environment does not emerge, the proposed system will not be able to be put into practice. However, if such technology does not emerge, there will be no digital rights management system and the problem of content providers having too much control over their copyrighted work will no longer exist as well.

Regarding the technology of issuing digital certificates, there is also concern that it may be subject to malicious attacks. Most security errors are due to implementation and management errors.[24] The Copyright Office may have its private key compromised because their employees do not follow closely the security procedure; there is no clear security procedure in place and they do not have enough resources and expertise to maintain the proposed electronic system. The employees within the Copyright Office may also feel uncomfortable about using a new technology and may make mistakes due

24 See Ross Anderson, *Why Cryptosystems Fail, University Computer Laboratory*, Cambridge, Britain, 1993

to a lack of understanding of the technology. As a result, the Copyright Office is advised to implement the proposed system to accept a limited amount of applications first so as to develop a clear and effective security procedure, before scaling up the system.

V. Trends

In the future, it will be impossible for the public to conduct non-infringing uses of copyrighted digital content. This section explains this trend by analyzing how the decentralized file-sharing system on the Internet, the new technology of digital rights management system and the Digital Millennium Copyright Act (DMCA) of 1998 lead to this result.

V.1 Overview

The combination of the digital technology and the widespread use of decentralized file-sharing system over the Internet enable the public to not only duplicate copyrighted digital work at practically no cost, but also distribute them over the Internet easily and quickly. Hence, it is hard for content providers to enforce their exclusive rights on their copyrighted work. They thus demand more protection of their content before they are willing to deliver it to their consumers. This demand of higher security on the Internet motivates software and hardware companies to develop digital rights management system. In 1998, Congress also passes DMCA, which criminalizes circumvention of technical means that control access to copyrighted work. As a result, content providers in the near future are likely to have the technological means as well as the legal support to determine all possible uses of their copyrighted work and eliminate any chances for the public to perform non-infringing uses with their work.

V.2 Decentralized File-sharing System and Digital Millennium Copyright Act

U.S. Court of Appeal for the Ninth Circuit, in the A&M Records, Inc. v. Napster, Inc. case ruled that Napster may be liable for contributory and vicarious copyright infringement. Napster used to be a free file-sharing service provider that allowed its users to swap files over the Internet. It is now in the process of changing its free service to a

subscription-base service.[25] This seems to be a manifestation of how the law has helped the content providers to enforce their exclusive right on their digital content. However, I argue that the content providers will still resort to technological means to guarantee the enforcement of their exclusive rights because of the introduction of decentralized file-sharing system, as compared to Napster's centralized one. Gnutella and Freenet are two examples of decentralized file-sharing system and while they allow users to swap files, yet they also have strong arguments against being charged for indirect copyright infringement.

Gnutella is a piece of open-source software that users can download free of charge from the Web. Gnutella forms a network, which overlays on top of the Internet and there is no central entity that owns the Gnutella network. When users swap files with other users, they do it without passing through any central entity. Gnutella's architecture is different from Napster's where a Napster user swaps a file with another user through a central server owned by Napster. As a result, although this Gnutella network may assist direct copyright infringement, content providers have no entities to sue for either contributory or vicarious infringement. The content providers can choose to go after the direct infringers – consumers, but that will be a public relations nightmare.

Freenet is also a piece of open-source software that users can download free of charge from the Web. It forms a distributed information storage and retrieval system, which makes enforcing copyright law impossible if some users obtain a piece of copyrighted work illegally and store it in the system. First, Freenet is designed to provide a high level of anonymity for producers and consumers of the stored information. It does so by restricting the knowledge of one user or a node in the system to its immediate neighbor.[26] Therefore, it is extremely hard for the content providers to find out who may be the direct and indirect infringers. Second, Freenet seals all the information it stores.[27]

---

[25] See John Borland, *Napster reaches settlement with publishers*, CNET News.com, September 24, 2001 at http://news.com.com/2100-1023-273394.html?legacy=cnet

[26] See Ian Clarke, *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, December 2000 at http://freenetproject.org/cgi-bin/twiki/view/Main/ICSI

[27] See Ian Clarke, *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, December 2000 at http://freenetproject.org/cgi-bin/twiki/view/Main/ICSI

Being unable to determine the content they store, Freenet users have strong defenses against indirect copyright infringement.[28] Third, Freenet propagates information it stores to some unknown nodes in the system every time someone requests that information[29]. Hence, if a piece of copyrighted work is illegally shared in the system, content holders will be unlikely to succeed in taking it out of the system and stop possible infringing uses. Forth, Freenet places all the functionalities of the system on the end users, so no central authority can shut down the system unless it occupies all the end nodes.[30] As a result, Freenet provides a technical infrastructure that prevents copyright holders to effectively enforce their exclusive rights.

All in all, decentralized file-sharing architecture such as Gnutella and Freenet compels content providers to look for a technical solution to enforce their exclusive right, rather than solely relying on the law. Although the Copyright Law may not be

---

[28] For more discussion, see Damien A. Riehl, Electronic Commerce in the 21st Century: Article peer-to-peer distribution systems: Will Napster, Gnutella, and Freenet create a copyright nirvana or gehenna? , William Mitchell Law Review, 2001

"Being able to deny any knowledge of the contents of one's machine might provide Freenet users with at least two defenses under [*1784] the Digital Millennium Copyright Act ("DMCA"). n142 In the DMCA, service providers are provided a "safe harbor" under which they are not held responsible for transitory digital network communications n143 and system caching. n144

Freenet users would likely fall under the "transitory digital network communications" category since the transmission was initiated by someone other than the user, the transmission was automated, the user does not select the recipients, and the material is not modified during the transmission. n145 There may be a question as to whether section 512(a)(4), which requires that the information not be "ordinarily accessible to anyone other than anticipated recipients," n146 is satisfied since others would subsequently be able to access the material.

An equally strong argument is that the mirroring of the information on a user's machine would constitute "system caching" under section 512(b). Freenet users also fall under this category since the users themselves are not accessing the information, but its location on their machines merely serves a caching function for other users. n147 One question is whether Freenet users adhere to Section 512(b)(2)(B)'s requirement that a user "complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol." n148 This may, however, be mitigated since such a protocol does not yet exist. n149

Like service providers, it is unlikely that Freenet users would be required to constantly police their systems for infringing content. Even more than service providers, Freenet users have the additionally high burden of decoding encryption to even determine whether the information on their system infringes upon a copyright. Since it is very difficult for users to determine the nature of the information stored on their systems, how can they be held responsible for its content and potential infringement?"

[29] See Ian Clarke, *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, December 2000 at http://freenetproject.org/cgi-bin/twiki/view/Main/ICSI

[30] See Ian Clarke, *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, December 2000 at http://freenetproject.org/cgi-bin/twiki/view/Main/ICSI

enforceable, law can still assist the content providers to secure their exclusive right by technological means and the Digital Millennium Copyright Act (DMCA) is an example.

Congress passed the DMCA in 1998, which mandates that no person shall circumvent a technological measure that effectively controls access to a work protected under 17 USC 1201. It provides content providers a legal support to criminalize entities who circumvent their protection technology that control access of their copyrighted work as well as entities who manufacture and offer to the public a device that is solely designed for circumvention of such technology. Hence, DMCA backs up content providers with legal power to employ a secure digital rights management system. Refer to Part III.2 for the details of a technical solution that is available for the content providers.

In summary, it is rational for content providers to look for a technological solution to protect their exclusive rights in light of the developments of digital technology and decentralized file-sharing system. Moreover, thanks to both the technology industry and the introduction of DMCA by Congress, they will have both the architecture as well as the law to employ strong digital rights management systems that protect their exclusive rights in the near future.

Conclusion

The widespread use of decentralized file-sharing systems compels digital content providers to demand a technical infrastructure that protects their exclusive rights. The introduction of DMCA further creates a legal framework for such technology. Software and hardware companies are also in line with the content providers in this endeavor and Microsoft Corporation has already obtained a U.S. patent on a digital rights management operating system that is able to identify software applications before loading them. This operating system therefore empowers the content providers to refuse delivering any copyrighted digital contents to their subscribers until the absence of software that the content providers dislike. As a result, the content providers are empowered to practically eliminate all possibilities for non-infringing uses of their digital work and effectively expand their exclusive right beyond the boundary defined in the Copyright Law. The

Copyright Office therefore should establish itself as a Certificate Authority who issues Digital Balance (DB) Certificates to software applications it deems compliant with the Copyright Law in order to re-open the door for the exercise of non-infringing uses of copyrighted work. Although the content providers have no legal obligation to honor the DB Certificates, the untouched and competitive market of online subscription and the norm of more liberal uses of digital content are likely to force them to do so. If the content providers instead of recognizing DB Certificates, choose other means to gain their market share, the introduction of DB Certificates still puts the government in a better position to create stricter regulation to limit the scope of copyright in the future. The introduction of Digital Balance Certificates creates a middle ground for both the copyright owners and the public to enjoy the benefits of the emerging digital era.