An Examination of Next-Generation Secure Computing Base and its Impact on Access and Control Rights

From Copyright Law to Technology—The Loss of Information in the Public Domain

Candidate Number: 446 370

Supervisor: Professor Olav Torvund

Delivered on August 15, 2003

Number of Words: 17,068

Table of Contents

Chapter 1: Introductory Remarks

1.1 Introduction

Increasingly over the past few years, with the explosion of the use of the Internet, there has been a move by copyright holders and content distributors to exercise control over works on the Internet through the use of code embedded in the works themselves. This change in the enforcement of copyright and the ways in which access to content is controlled has sparked a debate between copyright holders and those seeking to preserve the public's access to information.

Many of the recent changes in the field of intellectual property law have arisen as the result of advancements in digital technology and the widespread use of the Internet. The application of digital technology has changed the way in which content is reproduced and disseminated. Digital technology makes it possible to make virtually "perfect" copies of works at an extremely low cost. Working in conjunction with digital technology, the Internet enables these inexpensive nearly "perfect" copies to be distributed around the globe at record pace. Not everyone has welcomed this ability to obtain massive amounts of information in just seconds, 24-hours a day in a format that is virtually indistinguishable from the original. These changes in the way in which individuals are accessing and using information have rights holders worried.

Seeing digital technology as a threat, rights holders first sought to maintain their control over works through the increased use of click wrap contracts and licensing schemes. However, because the Internet is a highly decentralized network of networks that spans the globe, enforcement of intellectual property rights is extremely challenging in this environment. Lawrence Lessig states: "For the holder of the copyright, cyberspace appears to be the worst of both worlds—a place where the ability to copy could not be better, and where the protection of the law could not be worse."[1] Seeing the nearly impossible task of tracking and enforcing rights on a global scale, rights holders turned to technology itself as a means of protecting their works. In the words of Charles Clark, rights holders began to see that "The answer to the machine is in the machine."[2] Copyright holders and technologists began to explore ways in which technology could be used to preserve and even strengthen rights holders control over their works. These technologies have typically included password protection mechanisms, copy locks, conditional access systems, encryption techniques, and digital watermarking. Here, technology began to develop as a means of continuing to provide protection of intellectual property where the traditional protection offered under the law was weak. In this sense, technological measures became a "…privatized alternative to law."[3] However, because technology is developed by software engineers, and not legislatures, it does not necessarily conform to the protection offered by copyright law and the limitations contained therein. In some cases, the technology has been applied to bestow rights holders with more protection than is provided under copyright law.

This perceived expansion of intellectual property rights has caused controversy. Many fear that the traditional balance between the rights holder's limited monopoly on works and the public's right to information has become distorted with the imposition of technological protection mechanisms. Rights holders argue that without the ability to use technological measures they will have no meaningful mechanism by which to protect

[1] Lawrence Lessig, Code and Other Laws of Cyberspace, (New York: Basic Books, 1999), p. 125.
[2] C. Clark, "The answer to the machine is in the machine", The Future of Copyright in a Digital Environment (P. Bernt Hugenhotltz, ed., 1996), pp. 139-146.
[3] Lessig, Ibid., p. 130.

works in the online environment and that creators will cease to publish content in the digital format. In contrast, others opine that the intellectual property rights coupled with legal enforcement of technological measures are "…inconsistent with the preservation and growth of a vibrant public domain."[4] Furthermore, the increased use of technology to protect works frequently results in a loss of transparency that is provided for in the protection of copyright within a legal regime. Elizabeth Thornburg writes: "The Internet is largely a privatized world, and private actors are creating structures under which governments and their courts are increasingly irrelevant."[5]

1.2 Scope

This paper will examine the changing role of copyright in the digital age and the ways in which the use of technological measures and system development have impacted access to information in the public domain. This analysis will be made through the examination of new technology under development by Microsoft Corporation and the ways in which this technology may impact access rights and control over users. Specifically, the examination of the Next Generation Secure Computing Base Technology will be made under both the United States' Digital Millennium Copyright Act and the Copyright Directive and the E-Commerce Directive of the European Union. While the Next Generation Secure Computing Base (hereinafter referred to as "NGSCB") technology also raises questions in the areas of privacy, data protection, contract law, choice of law, and jurisdiction; these issues will not be discussed herein.

[4] Dan L. Burk and Julie E. Cohen, "Fair Use Infrastructure for Rights Management Systems", Harvard Journal of Law and Technology, Volume 15, Number 1, (Fall 2001).
[5] Elizabeth Thornburg, "Going Private: Technology, Due Process, and Internet Dispute Resolution", 34 UC Davis Journal of International Law and Policy 151, (2000): 153.

1.3 Research Methods and Materials

In assessing the impact of Microsoft's NGSCB technology on access and control rights an analysis was made of current treaties, including: the WIPO Copyright Treaty, the WIPO Performances and Phonograms Treaty, the Berne Convention, and the TRIPS Agreement. As a central aim of this paper is to compare and contrast the treatment of digital rights management systems or "trusted systems" in both the United States and the European Union. To this end, the following legislation is relevant: The Digital Millennium Copyright Act (DMCA), the Copyright Directive, and the E-Commerce Directive. Relevant cases interpreting the above mentioned legislation has been considered, and is discussed where appropriate.

In addition to analyzing the relevant legal instruments, an evaluation of numerous books, law review articles and corporate materials was made. Specifically, the technical and product specifications of the NGSCB project were obtained from Microsoft's website as well as the NGSCB website. Articles written by critics of the NGSCB project were primarily obtained using links contained on the Electronic Privacy Information Center website (www.epic.org). Assistance in understanding the technical aspects of the NGSCB project was provided by Gisle Hannemyr of the University of Oslo Department of Informatics. Furthermore, numerous articles and books by law professors, including Lawrence Lessig, Jessica Litman and Julie Cohen, focusing on digital rights management systems, technological measures, fair use, and trusted systems were also considered.

Chapter 2: Next Generation Secure Computing Base

2.1 What is Next Generation Secure Computing Base?

In May 2002, Microsoft announced that it had undertaken the development of technology to provide computer users with increased security and trustworthiness in the computing environment. The new features, to be integrated with the MS Windows Operating System, originally given the code name "Palladium" are now referred to as the Next-Generation Secure Computing Base (hereinafter referred to as "NGSCB"). This project is one of several that Microsoft has initiated as part of a broad based effort to increase security and reliability in the field of computing. In citing the need for increased trustworthiness in computing, Bill Gates states: "…it is the growth of the Internet and the advent of massive computing systems built from loose affiliations of services, machines, communications networks and application software that have helped create the potential for increased vulnerabilities."[6] Furthermore, Gates states: "…without a Trustworthy Computing ecosystem, the full promise of technology to help people and businesses realize their potential will not be fulfilled."[7] It is anticipated that these features may be available by as early as 2004. However, as applications, services, and content will need to become NGSCB enabled, widespread usage in the business environment may take some time.

2.2 Next-Generation Secure Computing Base Distinguished from TCPA

It is important to note that the NGSCB project is not Microsoft's implementation of the Trusted Computing Platform Alliance's specification version 1.1. The Trusted Computing Platform Alliance (TCPA), an industry working group, comprised of over

[6] Bill Gates, Executive Email, "Trustworthy Computing", (July 18, 2002), www.microsoft.com/mscorp/execmail/2002/07-18twc-print.asp.
[7] Ibid.

150 companies, is focused on improving trust and security on computing platforms.[8] The initiative was launched in 1995 by Compaq, Hewlett-Packard, IBM, Intel and Microsoft.[9] While the TCPA specification and NGSCB do share some common goals and features, their architecture is fundamentally different.[10] While both initiatives have the goal of creating a more secure computing environment, the architecture of the NGSCB is designed to promote a much broader functionality than TCPA. Microsoft has stated that it is currently working with the TCPA to develop a new TCPA specification that will meet NGSCB requirements.[11] Essentially, the TCPA technical specifications will exist as a subset of features that are incorporated into the NGSCB project.

2.3 Technical Details of the New Architecture

Prior to analyzing the legal ramifications of Microsoft's NGSCB for Windows project, it is necessary to understand the technical aspects of the product. To date, the project has been fraught with controversy about its technical capacity and the implications of implementing the new platform. In analyzing the product it becomes evident there is little actual disagreement over the technical capabilities of the project. Rather, the controversy stems from the product's capacity to not only improve system integrity and personal privacy, but also its ability to greatly limit users' access and control.

Microsoft describes the NGSCB for Windows project as a set of features that will enhance the Microsoft Windows Operating System by improving data security, personal privacy, and overall network integrity. This new system capability is designed to run in

[8] TCPA Frequently Asked Questions, Rev. 5.0, (July 3, 2002), www.tcpa.org, p. 1.
[9] Ibid.
[10] Microsoft Next-Generation Secure Computing Base – Technical FAQ, p. 6, www.microsoft.com/technet/security/news/NGSCB.asp?frame=true, January 12, 2002.
[11] Ibid., p. 6.

conjunction with the existing Windows Operating System and not underneath it thereby creating a virtually secure pc running alongside the traditional operating system.[12] Because the NGSCB project relies on new system architecture it requires changes to both hardware and software.

Specifically, the project will require changes to four essential components of the pc's hardware. Changes must be made to the central processing unit, the chipset (i.e. the motherboard), input devices such as keyboards, and video output devices such as graphics processors.[13] It is necessary that new secure input and output devices are incorporated so that user passwords and unprotected video signals cannot be detected by unauthorized individuals during an interaction between the CPU and any peripheral equipment. In addition, a new component comprised of a tamper proof secure cryptographic coprocessor will be required. It is envisioned that this component will be comprised of a tamper proof cryptographic smartcard containing unique cryptographic key pairs.[14] The smartcard module will, at a minimum, provide the RSA public key encryption operations of encryption, decryption, digital signature generation and verification, as well as AES encryption and decryption and SHA-1 hash computations.[15] The RSA private key and AES symmetric key are fixed and are not capable of being exported from the chip, thereby creating unique tracking possibilities.[16]

Microsoft is currently working with Intel and Advanced Micro Devices on the provision of a new x86 chip that will be used as part of the NGSCB platform. The x86

[12] Microsoft Next-Generation Secure Computing Base – Technical FAQ, (January 12, 2002), www.microsoft.com/technet/security/news/NGSCB.asp?frame=true, p. 2.
[13] Schoen, Seth, Palladium Details, ActiveWin, (July 8, 2002), www.activewin.com/articles/2002/pd.shtml.
[14] Ibid.
[15] Microsoft Next-Generation Secure Computing Base – Technical FAQ, Ibid., p 2.
[16] Ibid.

processor will enable the computer to boot in a new “trusted” mode and will permit cryptographically authenticated programs to access a separate memory area. The x86 processor will be augmented by the smartcard coprocessor that will hold the pair of unique cryptographic keys.

Software developed by Microsoft will work in conjunction with the hardware to enable the computer to operate in “trusted” mode. The software platform consists of the “nexus” or “trusted computing root” (TOR) and “nexus computing agents.”[17] The new operating system module will enable the secure interaction with applications, peripheral hardware, memory and storage.

Under the NGSCB, the trusted operating root and coprocessor work together to uniquely encrypt data so that no other trusted operating root/coprocessor combination, or the traditional MS Windows Operating System, will be able to decrypt the data or use the same signature keys. The nexus is essentially the kernel of an isolated software stack that runs alongside the existing software stack.[18] The nexus and nexus computing agents will operate simultaneously and in coordination with the underlying Windows Operating System.[19]

2.4 Operational Features

Microsoft cites four main categories of new security features that will be integrated into the NGSCB: protected memory, attestation, sealed storage, and secure input and output.[20] Protected memory is described as the ability to separate pages of main memory so that each application with NGSCB compatibility is protected from

[17] Microsoft Next-Generation Secure Computing Base – Technical FAQ, Ibid., p. 1.
[18] Ibid., p.2.
[19] Ibid.
[20] Ibid., p.1.

modification and so that its operations cannot be viewed by a third party. Attestation is referred to as the ability to digitally sign code or other personal data so that the recipient, or other software application, is assured that the code or data has originated from an unforgeable, cryptographically identified software stack. The sealed storage component is described as the ability of the computer to store information and applications in a cryptographically secure manner. Finally, the secure input and output category will ensure the safe interaction between the CPU and peripheral devices.

2.5 Next-Generation Secure Computing Base Benefits

Microsoft has identified three main categories where the NGSCB technology will prove beneficial to computer users. These three areas are: security, privacy, and system integrity. NGSCB will assist in the protection of information from interference or surveillance. The technology creates a secure environment in which computer code can run and information can be stored and processed without being viewed or captured by unauthorized individuals or even other programs resident on the computer or network.[21] Specifically, the technology is aimed at providing protection of data against malicious software such as viruses and Trojan horses, and at thwarting the use of spyware. While, virus software will still be needed for detection, with NGSCB technology, the virus protection software will be able to operate from a secure location on the hard drive. Thus, computers running NGSCB will essentially be protected from attacks by hackers unless the hacker has physical access to the individual machine.

The second benefit cited by Microsoft of the NGSCB technology is that it will increase personal privacy by preventing unauthorized personal data from entering the

[21] Microsoft Press Pass, Microsoft “Palladium”: A Business Overview, (June 18, 2003), www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp., p 2.

Internet or other network.[22] The technology will enable users to control the level of security that is used and determine the manner in which their personal information is released. Moreover, the technology will provide domain specific separation so that user errors are less likely to result in data leakage.[23]

Finally, the NGSCB will enhance overall system integrity by ensuring that computers, applications, and devices are properly verified before the user undertakes an interaction or engages in a transaction over the network.[24] This aspect of the technology, enabling the user to have cryptographic authentication between applications instead of between computers, is the main innovative achievement of the NGSCB project.[25] Robert X. Cringely describes the technology as "…essentially pasting a digital certificate on every application, message, byte, and machine on the Net, then encrypting the data… inside your computer processor."[26]

2.6 Criticisms of Next-Generation Secure Computing Base

In examining the NGSCB project it becomes evident that the technology should be viewed as a "toolbox" that has both the capacity to increase user security and privacy as well as the potential to restrict user access, control and privacy. While Microsoft has adamantly denied that they intend to apply the technology in these more sinister ways, it is these possible applications of the technology that have critics worried.

Many critics claim that the main application of the NGSCB project is as a digital rights management system. Digital rights management systems are defined as hardware

[22] Ibid., p. 2.
[23] Ibid., p. 2.
[24] Ibid.
[25] Boutin, Peter, "Palladium: Safe or Security Flaw", Wired News, www.wired.com/news/antitrust/0,1551,53805,00html.
[26] Cringely, Robert X., "I Told You So: Alas, a Couple of Bob's Dire Predictions Have Come True", I, Cringely, The Pulpit, www.pbs.org/cringely/pulpit/pulpit20020627.html.

and/or software systems that enforce a set of rules on the access and use of digital content or services.[27] Microsoft, however, denies that NGSCB is a digital rights management system.[28] Rather, they assert that NGSCB and digital rights management systems are two distinct technologies and that NGSCB merely facilitates the implementation of digital rights management systems.[29] Interestingly, the two patents covering the development of NGSCB describe the technology as a "digital rights management operating system."[30] Regardless of whether the NGSCB technology is characterized as a digital rights management system or not, it is clear that the project will facilitate a heretofore unprecedented level of access control over digitally distributed content.

Much of the criticism of the project focuses on the way NGSCB can be applied in order to control and potentially limit access. It is important to note that access control and copy control are two of the main features of any digital rights management system. A CNET article states that NGSCB will enable those in control of content, whether protected by copyright or not, to have the ability determine and enforce the conditions under which the material will be released. In this manner, NGSCB can be applied like a traditional technological measure that will enforce the conditions set by the content holder for distribution of the material. For example, a music download service could apply the technology to only permit download if payment had been made and the machine to which the material to be downloaded is also running on the NGSCB platform and has copy control mechanisms installed.[31] Furthermore, NGSCB is said to also

[27] Microsoft Next-Generation Secure Computing Base – Technical FAQ, Ibid., p. 7.
[28] Ibid.
[29] Ibid., p.8.
[30] Patent Number 6,330,670 and Patent Number 6,327,652.
[31] Lemos, Robert, "Trust or Treachery? Security Technologies Could Backfire Against Consumers", CNETnews, (November 7, 2002), www.cnetnews.com.

impose restrictions such as only permitting downloaded music to be played a specified number of times before requiring additional payment to the content provider.[32]

Moreover, many critics argue that NGSCB will have the ability to impose far more access and control restrictions than currently exist within other technologies. NGSCB is said to have a "policing mechanism" that will permit the automatic deletion of software and content.[33] For example, NGSCB could be applied to automatically destroy documents by "throwing away the digital keys" to a particular document after a specific period of time. Following corporate disasters such as Enron, Worldcom and Arthur Anderson, implications of such a technology are great. Additionally, many critics fear that NGSCB could be applied to censor works that criticize the government or even Microsoft.

Even more potentially threatening is NGSCB's ability to automatically delete content that a rights holder claims is infringing on his or her copyright. With the ability to automatically delete content on a global scale from a single remote location, the transparency that exists in the current legal regime is lost and instead control is transferred from legislatures and judicial systems to individuals and corporations in the private sector. The ability of NGSCB to facilitate remote deletion can be accomplished regardless of jurisdiction rules and whether or not there is an underlying copyright violation. Furthermore, as with other technologies, NGSCB serves to shift the burden of proving that a use is noninfringing onto individual users who may not possess the financial means or jurisdictional reach to pursue a claim against a rights holder.

[32] Anderson, Ross, *TCPA/Palladium FAQ's*, www.epic.org.
[33] Lemos, Ibid.

Furthermore, when NGSCB is operating, the computer will automatically verify all hardware and software during "boot up". This enables the technology to be used to automatically prohibit access to any software for which the license has expired or been revoked. While the ability of NGSCB to detect and automatically remove "pirate" software is an enormous innovation in the enforcement of copyright, this feature also potentially results in a user's access to documents he or she created being blocked if the software license has expired or been revoked. This aspect of NGSCB demonstrates the way those who control technology also direct access to and control over derivative works.

Moreover, because as an operating system, NGSCB will have the ability to determine which applications it will run, it is said to have the potential to dramatically harm the open source movement.[34] Some critics claim that because the NGSCB requires the signing of software the open source movement will be harmed in that open source promotes the modification of code and that each modification will require a new signing in order to become NGSCB compliant. Because NGSCB is said to withhold the cryptographic keys from users it places Microsoft as the gatekeeper of verification and authentication. It is for these reasons, that Richard Stallman has referred to the NGSCB project as enabling not "trusted computing", but rather enforcing "treacherous computing" because it will permit your computer to systematically disobey you.[35]

It is important to note that Microsoft has claimed that users will retain the choice of whether to run NGSCB and that the product will be shipped with the features disabled. However, over time, users could be forced to run NGSCB if it is widely adopted by e-commerce sites and distributors of content on the Internet. If NGSCB does develop into

[34] Lemos, Ibid.

[35] Stallman, Richard, Ibid.

an “industry standard”, the fact that a user can technically disable NGSCB will be of little importance since his or her ability to access content on the Internet will be severely limited by the requirement that users run NGSCB in order to access content.

With NGSCB’s ability to severely limit user access and control, it becomes imperative to explore whether there are, within the existing legal regime, adequate measures to protect users from potentially invasive actions and to assist in maintaining the balance that exists within copyright law.

Chapter 3 Evaluation of NGSCB as a Technological Measure

3.1 Introductory Remarks

With NGSCB’s apparent ability to be applied to limit and control a user’s access to content on the Internet, and access to one’s own content, it becomes imperative to evaluate and assess whether there are any existing legal regulations that will prevent NGSCB from being applied in these nefarious ways. Specifically, it is important to evaluate whether a user will be permitted to employ technology directed at disabling or circumventing the technology that makes the limitations on user access and control possible under NGSCB.

3.2 Legal Protection of Technological Measures—WIPO Treaties

In 1996 the World Intellectual Property Organization (WIPO) enacted the Copyright Treaty[36] and the Performances and Phonograms Treaty.[37] The WIPO Copyright Treaty provides international protection of copyrighted material to the extent

[36] World Intellectual Property Organization (WIPO) Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/94.

[37] World Intellectual Property Organization (WIPO) Performances and Phonograms Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/95.

provided under the Berne Convention. The WIPO Performances and Phonograms Treaty gives sound recordings protection similar to that provided under the Berne Convention. However, the WIPO treaties went far beyond providing protection of copyrighted material, and also included provisions to protect the technology that was increasingly being used by rights holders to protect their works. This change, requiring member countries to provide legal remedies and protection against circumvention of technological protection measures that are used by creators, serves to provide a legal endorsement and protection for the technologies employed by rights holders. Specifically, Article 11 of the WIPO Copyright Treaty provides: "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[38] The implementation of Article 11 of the WIPO Copyright Treaty in the United States was codified in the Digital Millennium Copyright Act (DMCA) and in the European Union in the Copyright Directive.[39]

3.3 Digital Millennium Copyright Act (DMCA)

The DMCA[40] contains both content and technology related provisions and was enacted in order to comply with the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The purpose of the DMCA is to bring the protection and

[38] World Intellectual Property Organization (WIPO) Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/94.

[39] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

[40] Digital Millennium Copyright Act, enacted October 20, 1998, Title 17 United States Code.

enforcement of copyright "squarely into the digital age."[41] In fact, the United States played a central role in pushing for the adoption of the WIPO treaties. Like their counterparts in Europe, the United States felt that without strong copyright protection e-commerce would not fully develop into a vibrant on-line marketplace where "…via the Internet the movies, music, software and literary works that are the fruit of American genius"[42] would be available. Unlike previous U. S. legislation protecting intellectual property rights, however, the DMCA was unique in that it contained protection of technology aimed at protecting copyright as well as protecting the underlying works themselves.

3.3.1 Anti Circumvention Provisions of the DMCA

The DMCA contains three provisions aimed at prohibiting circumvention of technological measures that are employed to protect a work. Section 1201(a)(1)(a) sets forth the basic rule prohibiting circumvention of technological measures that control access. Section 1201(a)(2) provides a prohibition on the trafficking of devices aimed at circumventing access control technological measures. Lastly, Section 1201(b) prohibits the trafficking in devices aimed at controlling copying of protected works. Thus, the DMCA includes provisions aimed at both the act of circumvention and the trafficking in devices designed to circumvent technological measures. However, it is important to note in order meet the burden of proof for a violation of the anti-circumvention provisions "…a finding of copyright infringement is not necessary."[43] Rather, a violation of the anti-circumvention provisions is a distinct violation and exists regardless of whether there

[41] Report of the Senate Committee on the Judiciary, S. Rep. No. 105-190, (1998), p. 2.

[42] Ibid.

[43] Fallenböck, Markus, "On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions", International Journal of Communications Law and Policy, Issue 7, (Winter 2002/2003), p. 13.

is an underlying infringement of copyright. This raises the question of whether or not Section 1201(a)(3)(b) can be invoked against a user who employs circumventing technology to gain access to a work that is not protected by copyright. This issue will be addressed in Section 3.3.6 contained herein.

3.3.2 Section 1201(a)(1)(a)

Section 1201(a)(1)(a) states that: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[44] Moreover, Section 1201(a)(3)(a) defines "to circumvent a technological measure" as: "to descramble a scrambled work, to decrypt an encrypted work, or otherwise avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner…."[45] Furthermore, a technological measure is deemed "effective" if "the measure, in the ordinary course of its operation requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to a work."[46] It is important to note that the provision prohibiting the act of circumvention only relates to access controls that have been applied to a work and does not relate to the act of circumventing copy control mechanisms. Furthermore, the ban on the act of circumvention exists independent of whether the underlying use of the work is legitimate and regardless of any defenses that may be applicable.[47]

Section 1201(a)(1)(a) was subjected to a two-year moratorium on implementation while the Librarian of Congress assessed the impact of the provision on users ability to

[44] Title 17 United States Code Section 1201(a)(1)(a).
[45] Title 17 United States Code Section 1201(a)(3)(a).
[46] Title 17 United States Code section 1201(a)(3)(b).
[47] Fallenböck, Markus, Ibid., p. 14.

continue to make non-infringing uses of protected works.[48] Section 1201(a)(1)(b) states: "The prohibition…shall not apply to persons who are users of a copyrighted work which is in an particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works…."[49] As the statute does not provide a definition of "a particular class of works", this became a central point of debate with proponents of fair use arguing for "class" to be defined by the use to which the work was made and by copyright owners arguing for a narrow interpretation.[50] The Librarian of Congress, following a review of the legislative intent of the statute concluded: "that a 'class' of works has to be defined, primarily, if not exclusively by reference to attributes of the works themselves."[51] To date, the Librarian of Congress has issued a few narrowly defined exemptions. It is important to note, however, that while certain exemptions may be granted for the act of circumvention of access controls, use of technologies aimed at circumvention of access or copy controls is still not permitted.

3.3.3 Section 1201(a)(2)

Section 1201(a)(2) provides that: "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

[48] Title 17 United States Code Section 1201(a)(1)(b).
[49] Title 17 United States Code Section 1201(a)(1)(b).
[50] Fallenböck, Markus, Ibid., p. 22.
[51] Ibid., p. 23.

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."[52] Here, the same definitions of "circumvention" and "effective" apply as in Section 1201(a)(1)(a). Moreover, as with the prohibition of the act of circumvention, a defendant is precluded from arguing that the underlying use of the circumvention technology was to facilitate a use that is permitted by copyright law.

Section 1201(a)(2) is tempered in that only devices with a "limited commercially significant purpose" are prohibited. According to Markus Fallenböck, "…it is not aimed at products that are capable of commercially significant non-infringing uses, such as consumer electronics, telecommunications, and computer products – including videocassette recorders, telecommunications switches, personal computers, and servers – used by businesses and consumers for perfectly legitimate purposes.

3.3.4 Section 1201(b)

Section 1201(b)(1) details the prohibition on the trafficking in devices designed to circumvent technological measures aimed at protecting against unauthorized copying. Specifically, Section 1201(b) states: "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, or component, or part thereof, that – (a)is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or portion thereof; (b) has only a limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner

[52] Title 17 United States Code Section 1201(a)(2).

under this title in a work or a portion thereof; or (c)is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof."[53] While the wording of Section 1201(b) is similar to that in Section 1201(a)(2), it differs in that it is aimed at protecting the creator's underlying rights in copyright. Thus, Section 1201(b) is "…subject to the limitations of the Copyright Act while the protections against unauthorized access are not."[54] The DMCA does not provide a provision similar to Section 1201(a) that prohibits the act of circumventing copy control technological measures. Fallenböck asserts that: "The prohibition on circumvention activities in the basic provision is necessary because prior to the DMCA, the conduct of circumvention was never before made unlawful. The ban on access-circumvention devices enforces this new prohibition. In contrast, the copyright law has long forbidden copyright infringements, so no new prohibition was necessary."[55]

3.3.5 Exemptions under the DMCA

While not within the scope of this paper, it is important to note that the DMCA provides several exemptions to the ban on circumvention. Permitted actions include circumvention for the purposes of: nonprofit libraries, archives, and education institutions assessing whether to acquire a work, law enforcement for investigative and security purposes, reverse engineering in order to obtain interoperability and to test system security, encryption for purposes of encryption research, for the protection of

[53] Title 17 United States Code Section 1201(b).

[54] Fallenböck, Markus, Ibid., p. 17.

[55] Ibid., p. 22.

[55] Ibid., p. 18.

minors, and for the protection of personally identifying information. However, some of the exemptions only permit the act of circumvention while the prohibitions on the use of devices aimed at circumvention remain in effect. This potentially prevents a user who falls within a protected class from effectively being able to exercise their right to circumvent.

3.3.6 Judicial Interpretation of the Anti-Circumvention Provisions

In 2000, the first legal challenge to the anti-circumvention provisions of the DMCA was raised in Universal City Studios, Inc. v. Reimerdes (111 F. Supp 2d 346). This case concerned the cracking of the Content Scramble System (CSS). CSS was an encryption technology used by the Digital Versatile Disk (DVD) industry to ensure that DVD movies could only be viewed on machines that had been licensed to decrypt CSS. Prior to 1999, decryption licenses for CSS had only been granted for Windows and Macintosh compatible computers.[56] Machines operating on the Linux platform were not licensed to decrypt CSS and hence, were unable to play DVD movies. It is important to note, however, that CSS did not prevent the copying of DVD movies, but rather only limited the types of machines that could be used to play DVD movies.

In September 1999, Jon Johansen, a Norwegian teenager, decrypted CSS and wrote a program to decrypt CSS, aptly named DeCSS, so that DVD movies could be played on machines running Linux (or other operating systems). Jon Johansen then posted the executable object code for DeCSS on his website. Within weeks, the DeCSS decryption program was posted on websites throughout the world and several lawsuits

[56] Lawrence Lessig, The Future of Ideas: The Fate of the Commons in a Connected World, (New York, Vintage Books, 2002), p. 189.

were filed by the DVD industry seeking injunctions to stop the distribution of the program.

The main case concerning DeCSS was tried in New York and resulted in temporary and permanent injunctions being issued enjoining the defendants from posting the DeCSS program and from linking to other websites where the program was posted. Interestingly, none of the several defendants was engaged in the selling or distribution of "pirate" DVD movies. In fact, the plaintiffs never proved that any "pirate" DVD movies had been distributed because of DeCSS. Rather, the plaintiffs claimed that the posting of the DeCSS program constituted a violation of the anti-circumvention provisions of the DMCA.

One of the numerous defenses claimed by the defendants was that the "fair use" limitation on copyright granted them the right to post and distribute DeCSS. However, this argument was rejected by the lower court and affirmed on appeal. The court held that the "fair use" argument was without merit as the defendants' actions could be enjoined under the anti-circumvention provision of the DMCA and this provision ". . . does not concern itself with the use of those materials after circumvention has occurred."[57] Lawrence Lessig, referring to this case, states: "Fair use, the court concluded, was something that copyright law must allow. This was a law regulating code, not a copyright. The court concluded that Congress has the power to allow private actors to pile on protection on top of the copyright law."[58]

With the court clearly rejecting the "fair use" argument as providing permission to circumvent technological measures and the statement that the anti-circumvention

[57] Universal City Studios, Inc. et al. v. Eric Corley, United States Court of Appeals for the Second Circuit, Docket No. 00-9185, Decided November 28, 2001, p. 8.
[58] Lessig, Ibid., p. 190.

measures are only concerned with the act of circumvention and the technology that is used rather than whether the purpose of circumvention was to avail oneself of a copyright limitation, one wonders whether the anti-circumvention provisions could also be applied where an individual uses circumvention to gain access to a work not protected by copyright. In the DeCSS case, the court briefly considered this issue since it was raised in an amici curae brief submitted in support of the defendants by forty-five law professors. However, the court found that this issue was outside the scope of the current action since DVD movies were clearly protected by copyright. The court stated: ". . . the possibility that encryption would preclude access to public domain works 'does not yet appear to be a problem, although it may emerge as one in the future.'"[59] Thus, the question remains unanswered. However, with the broad interpretation of the anti-circumvention provisions by the court in the DeCSS case it does not appear impossible that a court could find a violation of the anti-circumvention provisions even if the circumvention was accomplished to gain access to a work in the public domain.

Another interesting aspect of the DeCSS case is the broad interpretation of the access anti-circumvention provision used by the court. The court found that the provision was violated even though DeCSS was to be used to simply view DVD movies on another operating system. Presumably, an individual would have lawfully purchased a DVD movie and would use DeCSS to view the movie on a machine using Linux. Here, the court held that although the purchaser had a lawful right to access and view the DVD movie, by virtue of the fact that they had purchased the DVD, the user, by electing to view the DVD on a machine that was not licensed, subsequently violated the anti-circumvention provisions. Thus, the court appears to endorse the idea that even though a

[59] Ibid., p. 9.

user may have an initial right of access, by electing, subsequently to access content in a manner not approved by rights holder he or she violates the anti-circumvention provisions. Some have argued that this interpretation of Section 1201 is not supported by the legislative history of the DMCA.[60] Furthermore, the standard to be used to judge circumvention technology is "capable of commercially significant non-infringing uses". Here, the ability to view DVD movies on computers running Linux appears to be a "commercially significant non-infringing use".

3.4 The European Copyright Directive Union

The WIPO Copyright Treaty Article 11 provisions relating to technological measures are codified in the European Union's Copyright Directive.[61] Like the DMCA, the Directive prohibits both the act of circumvention and preparatory acts related to circumvention. Article 6(1) of the Directive states: "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective."[62] The prohibition against circumvention devices is contained it Article 6(2) which states: "Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which: (a)are promoted, advertised or marketed for the purpose of circumvention of, or (b)have only a limited commercially significant purpose or use other than to circumvent, or (c)are primarily designed,

[60] Fallenböck, Ibid., p. 19.
[61] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.
[62] Ibid., Article 6(1).

produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measure."[63]

Moreover, the Directive defines the term "technological measures" as well as the term "effective". Article 6(3) defines technological measures as "…any technology device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the rights holder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for. . ." in the database directive.[64] Furthermore, a technological measure is: ". . . deemed 'effective' where the use of a protected work or other subject-matter is controlled by the rights holders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective."[65]

3.5 Comparison of the DMCA and the Copyright Directive

As both the DMCA Section 1201 and the Copyright Directive Article 6 provisions are implementations of the WIPO Copyright Treaty Article 11, they have some similarities. However, there are also distinct differences in the manner in which the implementation of Article 11 was accomplished.

Both the DMCA and the Copyright Directive provide more protection against circumvention than was envisioned in the WIPO Copyright Treaty. This is evidenced by the provisions in both the DMCA and the Copyright Directive that prohibit trafficking in

[63] Ibid., Article 6(2).
[64] Ibid., Article 6(3).
[65] Ibid.

devices that can be used for circumvention.[66] Fallenböck opines: "Both acts are based on the notion that the real danger for intellectual property rights will not be the single act of circumvention by individuals, but the preparatory acts carried out by commercial companies that could produce, sell, rent, or advertise circumvention devices."[67] Both the DMCA and the Copyright Directive require that the technological measure be "effective" and they similarly define "effectiveness".

A central difference between the DMCA and Copyright Directive exists in the provisions that prohibit the act of circumvention. While the DMCA appears to be limited to ban the act of circumvention as it relates to access controls, the Copyright Directive contains no similar limitation.[68] Rather the Copyright Directive merely uses access control as an example of a technological measure. While the DMCA Section 1201 only prohibits the act of circumventing access control technological measures, the Copyright Directive bans acts of circumvention of both access and copy control technological measures.[69]

Another main difference between the DMCA Section 1201 and the Copyright Directive Article 6 is evident through an examination of how the protection of technological measures relates to copyright infringement. The DMCA provision banning circumvention of access control mechanisms exists as an unlawful act that is separate and distinct from any underlying copyright infringement and exclusive of any privilege or defense that could be asserted to excuse the unauthorized use of the work. Fallenböck asserts: "One of the most criticized features of Section 1201 of the DMCA, is that it

[66] Fallenböck, Markus, Ibid., p. 38.
[67] Ibid.
[68] Ibid., p. 39.
[69] Ibid., p. 40.

prohibits circumvention whether or not the underlying use is privileged."[70] Indeed, this was the position adopted by the court in the DeCSS case. While the Copyright Directive is not entirely clear, it appears to prohibit circumvention as it relates to an underlying copyright infringement.[71] Article 6(3) of the Copyright Directive defines technological measures as those designed to protect against copyright infringement, related rights, and the sui generis rights for databases. Furthermore, Article 6(4) directs Member States to ensure that certain exceptions and limitations to the exclusive rights of copyright holders are not barred by the imposition of technological measures.[72] Thus, it appears that Member States are directed to ensure that limitations on copyright such as: copying for private use, use by educational institutions, libraries, and researchers, and use for purposes of criticism are not unduly impacted by Article 6.

However, the implementation of the provisions contained in Article 6(4) has varied widely in Member States. For example, in Austria, the implementation 6(4) is not included in the legislation.[73] Huppertz states: "…this seems to indicate that the Minister of Justice does not consider the actual situation on the Austrian market regarding access to works under the exceptions listed in that Article as requiring an intervention from the public authorities and leaves it to the market place to develop negotiated solutions."[74] In the Netherlands, the implementation of Article 6(4), contained in Article 29a of the

[70] Ibid.
[71] Ibid., p. 41.
[72] Ibid., Article 6(4).
[73] Marie-Thérèse Huppertz, "The Pivotal Role of Digital Rights Management Systems in the Digital World—An analysis of the copyright protection provided for in the 2001 Copyright Directive with a specific emphasis on the protection of the digital rights management systems and their implementation into the national law", Cri 4/2002, p. 109.
[74] Ibid.

Copyright Act, allows "…competent authorities to adopt the necessary measures, but does not list the measures that should or might be taken."[75]

Both the DMCA and the Copyright Directive raise the conflict between the need to strengthen rights holders' protection against piracy and users' rights to access and use material as provided by the exceptions and limitations within copyright protection. The interaction between technological protection and fair use and private copying will be considered in Chapter 5. However, it is first necessary to evaluate the NGSCB technology as a technological measure under both the DMCA and the Software Directive.

3.6 Evaluation of NGSCB as a Technological Measure

In examining whether the NGSCB technology will be considered a technological measure, it is imperative to consider both Microsoft's stated product uses as well as the other potential uses put forward by critics of the project. One stated objective of NGSCB put forth by Microsoft is that it will improve security and system integrity by providing cryptographic authentication between applications. Furthermore, Microsoft has indicated that NGSCB will facilitate the implementation of pay-per-use digital rights managements systems. If one assumes that the statements put forth by critics of NGSCB are correct, NGSCB also has the ability to greatly control access and uses to which works are put by imposing access and copy restrictions on works, regardless of whether the works themselves would be entitled to copyright protection or the use would fall within an established limitation to intellectual property rights. While Microsoft asserts that the NGSCB will be shipped with the features turned off, content owners and distributors running NGSCB can insist that content will only be released to others who are also using the NGSCB platform with the access and copy control features in place. It is then

[75] Ibid., p. 111.

necessary to determine what, if any, protection NGSCB will have as a technological measure and what the implications will be if a user acts to circumvent the restrictions imposed by NGSCB.

3.6.1 NGSCB and the DMCA Section 1201

As Section 1201 prohibits both the act of circumvention of access control technological measures as well as the trafficking in devices aimed at both access and copy control, and the NGSCB technology contains features aimed at controlling access and limiting unauthorized copying, it will fall within the parameters of Section 1201. Moreover, Section 1201(a)(3)(a) defines a technological measure as one that is capable of, among other things, encryption. The central feature of NGSCB is that it is capable of encryption between applications.

Next, it is necessary to evaluate whether the access and copy control mechanisms meet the "effectiveness" criteria as established in Section 1201. "Effectiveness" is said to exist, under Section 1201(a)(3)(b) if the technological measure, when used in its normal course of application, requires the authority of the copyright owner to gain access. One of the stated features of NGSCB is that it is capable of enforcing restrictions related to the release of information over a network, such as the Internet.

Furthermore, as Sections 1201(a)(2) and 1201(b) relating to the trafficking of anti-circumvention devices utilize the same definition of "technological measure" as Section 1201(a)(1)(a), it appears that a device created to circumvent both the access and copy control features of the NGSCB would be prohibited provided the device has only a limited application other than circumvention or unless the purpose for circumvention fell within one of the stated exceptions to the DMCA. However, if an individual circumvented NGSCB for a purpose falling within "fair use", he or she could not raise that as a defense to escape liability under Section 1201.

3.6.2 NGSCB and Article 6 of the Copyright Directive

As under the DMCA, the NGSCB technology seems likely to be covered under Article 6 of the Copyright Directive. As NGSCB includes features designed to prevent and restrict acts that are not authorized by the rights holder, it meets the definition of "technological measures" set forth in Article 6(3). Like the DMCA, Article 6 requires that technological measures be "effective" in order to benefit from the protection offered therein. Again, access and copy control mechanisms are cited as examples of "effective" technological measures. However, unlike under the DMCA, a user who circumvents NGSCB for the purpose of exercising his or her rights under the private copying limitation may be able to escape liability as Article 6 seems to imply that an underlying copyright infringement is necessary in order to establish liability under Article 6.

3.7 Summation of Chapter 2

It seems evident that the NGSCB technology will meet the standards set forth for protecting technological measures under both the DMCA and the Copyright Directive. However, since one hallmark of the NGSCB project is that it imposes restrictions and controls access to works, it is necessary to evaluate the impact that such restrictions will have on the availability of information in the public domain. Specifically, it is important to analyze the impact that NGSCB technology may have on the intermediary liability procedures set forth in the DMCA and the E-Commerce Directive.[76] The ways in which NGSCB technology may impact the transparency provided for under the current legal

[76] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce. Hereinafter referred to as the E-Commerce Directive.

regime and the movement towards privatization of law in this field will be explored in the next chapter.

Chapter 4: NGSCB's Impact on Intermediary Liability

4.1 Introductory Comments

The implementation of NGSCB will have a dramatic impact on the legal rules regulating intermediary service provider liability. If the NGSCB critics are to be believed, NGSCB's ability to remotely delete content will render the rules on intermediary service provider liability, both under the DMCA and the E-Commerce Directive, virtually useless. While both the DMCA and the E-Commerce Directive regulations have been criticized, the result if NGSCB is implemented will be far worse. Prior to analyzing how NGSCB will impact these regulations, it is first necessary to examine the current regulations.

4.2 DMCA's "Notice and Take Down" Procedures

The rules governing intermediary service provider liability are codified in Title II of the DMCA. Section 512 of the Copyright Act establishes four limitations on copyright infringement for on-line service providers. These limitations include exemptions from liability in the following circumstances: 1)transitory communications, 2)system caching, 3)storage of information at the direction of a user, and 4)information location tools (i.e. search engines). In order for the exemptions stated in Section 512 to apply, a service provider must comply with two main requirements. First a service provider must implement a policy that provides for the termination of user accounts when the user repeatedly violates provisions of the DMCA. Additionally, in order to claim the exemptions under Title II, a service provider must not interfere with "standard technical measures" employed by rights holders to protect their works. Standard technical measures are defined as those that 1)copyright owners use to identify or protect copyrighted works, 2)have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair and voluntary multi-industry process, 3)available to anyone on reasonable nondiscriminatory terms and 4)do not impose substantial costs or does not burden service providers.[77] Under the DMCA, the service provider is under no obligation to monitor content.

In order for a service provider to avail itself of the "safe harbor" provisions, it must comply with the established notification procedures set forth in the DMCA. The notification procedure requires the service provider to remove allegedly infringing material upon notification by the rights holder. The notification must include the following information: 1)physical or electronic signature of the rights holder or a person legally authorized to act on the rights holder's behalf, 2)it must identify the infringing material in a manner sufficiently detailed as to enable the service provider to identify it, 3)sufficient contact information, 4)a statement executed under penalty of perjury that the party providing notice has a good faith belief that the material is infringing, and 5)a statement that the information contained in the notice is correct.[78] Upon receipt of a notification containing the required elements the service provider is required to remove the allegedly infringing material and notify the user of its removal.

Section 512(g) provides for a counter notification procedure if the user believes that the removal of the allegedly infringing material is improper. If the service provider receives a counter notification then it must replace the material that has been removed

[77] 17 U. S. C. 512(i).

[78] 17 U. S. C. 512(c)(3).

within ten to fourteen days unless the rights holder provides proof that a court action has been filed to resolve the infringement issues.

If the service provider complies with the procedure set forth in the DMCA then the service provider will be immune from claims of both vicarious and contributory copyright infringement. Furthermore, if it is later discovered that the service provider removed material that was not infringing based on a notice claiming infringement, the service provider will still be permitted to take advantage of the "safe harbor" provisions.

4.3 Intermediary Liability in the European Union

Prior to the implementation of the E-Commerce Directive on January 17, 2002, Member States had widely varying laws that regulated service provider liability. Because of the plethora of legal rules and because widely differentiated results cases involving service provider liability were harming the Internal Market, the E-Commerce Directive was developed and adopted as a means of harmonizing liability rules.

The liability limitations and exclusions for on-line activities are contained in Articles 12 through 15 of the E-Commerce Directive. Like the DMCA, the Directive exempts service providers from liability for activities that include: 1)mere conduit, 2)caching, and 3)hosting. However, unlike the DMCA, the E-Commerce Directive does not provide a liability exemption for search engines or other information location tools that compile information for the benefit of the user. Like the DMCA, the E-Commerce Directive does exempt the service provider from civil and criminal liability, but does not protect the service provider from liability for material that has been created or modified by the service provider. As with the DMCA, the E-Commerce Directive states that service providers are under no obligation to monitor information that they store or transmit.[79]

Unlike the DMCA, which provides a "safe harbor" for service providers who remove allegedly infringing material upon notification, the E-Commerce Directive uses a "knowledge" standard. Under the E-Commerce Directive, a service provider will be liable if the provider has actual knowledge of facts and circumstances from which illegal activity is apparent and does not act expeditiously to remove the illegal material.[80] The use of a "knowledge" standard as opposed to setting forth an explicit procedure that directs service providers to remove allegedly infringing information has been criticized as providing an incentive for service providers to remove material upon any notification of potential infringing information.[81]

4.4 NGSCB's Impact on Intermediary Liability Rules

While both the DMCA Title II and the E-Commerce Directive have been criticized as shifting the procedural advantage from users to rights holders and for employing a not particularly transparent, quasi-privatized form of law; the impact that may be caused upon the implementation of NGSCB is far more dramatic.

The concerns over the existing legal rules are said to create an incentive for service providers to be overly cautious in removing allegedly infringing material so that they may escape liability. In this sense, on-line providers become the enforcers of

[79] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), Article 15.

[80] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), Article 13(1)(c) and Article 14(1) subsections (a) and (b).

[81] Rosa Julià-Barceló, "Section 4: Intermediaries: Ch. 1: Liability for on-line Intermediaries: Comparing EU and US Legal Frameworks," (Walden, Ian & Hörnle, Julia, editors, Woodhead Publishing Limited 2001), p. 13.

copyrighted material for rights holders.[82] With the current regulatory regime, the burden of proving that posted material is not infringing shifts to the user. These rules are a dramatic move from the traditional requirement that a rights holder must prove infringement. Furthermore, the service provider liability exemptions amount to the equivalent of granting a preliminary injunction without application of the law and often without requiring the rights holder to personally interact with the alleged infringer.

Furthermore, the exemption for on-line service providers creates a quasi-privatized form of law that lacks transparency. If one envisions an individual user who has posted allegedly infringing material on their personal homepage, it becomes apparent that the user may not have the time or financial resources to pursue an action in court to prove that the material is non-infringing or falls within a copyright limitation. While in the United States, the possibility of filing a class action lawsuit exists, most likely, unless the action by the rights holder to remove the material occurs on a mass scale, the user will essentially be left without a remedy. Moreover, a European user will, most likely, be left without a remedy since class action lawsuits are generally not permitted in the European Union.

As potentially harmful as the current service provider exemptions are, the results, if NGSCB technology is widely implemented, will be far worse. If the claims asserted by NGSCB's critics are correct and access to material can be blocked or deleted remotely by the holders of the cryptographic keys, then rights holders will possess the power to automatically enforce their views of what constitutes copyright infringement. Going even further, the holders of cryptographic keys will be able to remotely delete material that expresses an unpopular political view or is critical of a particular individual or

[82] Thornburg, Ibid., p. 171.

corporation (e.g. Microsoft). It is in this situation that the importance of permitting the user to have access to the cryptographic key pairs used by them in creating material becomes evident.

Using the same example cited above of a user posting material to his or her personal website, the rights holder claiming infringement will have the ability to remotely delete the material. Here, the deletion can occur without notice and in secret. With the possibility of automated deletion, the user is deprived of his or her due process rights regarding notice and access to the courts. The benefit of the current regulatory regime is that, at a minimum, the established procedures require notice to the affected user and create a written record that may be later used in court. With NGSCB, the important benefits provided by written notification are lost.

The widespread application of NGSCB can also be used to automatically and remotely delete content in situations where the intermediary liability rules would not apply. For example, NGSCB can be used to automatically delete content of a work that does not meet the standard for copyright protection. Here, the application of technology can be used to control access to information that was never intended to be subjected to the "limited monopoly" granted by copyright law. Furthermore, NGSCB may prove to be beneficial to governments who wish to prevent information from being available in the public domain. Typically, government documents are not eligible for copyright protection. However, through the application of NGSCB technology and by virtue of the work existing in a digital format, the government can block access to government works. While a user seeking access may be able to eventually gain a right of access following a court decision under "freedom of information" legislation, such a result will take time and, most likely, substantial financial resources. Here, the application of NGSCB technology will, at very least, assist the government in temporarily blocking access to information. Such actions clearly do not comport with traditional notions of democracy.

As discussed in the chapter on technological measures, the "automatic deletion" functionality of NGSCB represents yet another example of the ways in which enforcement through technology can provide greater enforcement power than that provided under the law. Beyond the expansion of enforcement powers, we see an increased loss in transparency that operates to the detriment of users and the general public. If the intermediary liability rules are to remain, new legislation should be introduced that requires compliance even if technology exists that can circumvent the intermediary.

Chapter 5: Impact on the Public Domain

5.1 Introductory Comments

The combination of the increased use by rights holders of technology to protect their works, the prohibition on employing circumvention technology, and the "safe harbor" provisions for on-line intermediaries has shifted the focus of copyright from limiting the use of protected works to control over access. This represents a growing divergence between the legal rules applicable to traditional media and the rules applied to digital products. Hugenholtz has argued that the appeal of using technology to limit access from a rights holder's perspective is that it "…leaves the user no alternative but to comply (cheap and fast) 'self-enforcement' instead of (expensive and slow) enforcement by the law."[83] It is this ability of creators to absolutely control the use of their works,

[83] Bernt P. Hugenholtz, Ibid., p. 315.

independent of the law, which fuels the debate over fair use and private copying. In addition, it is stated that "…anticircumvention provisions encourage copyright owners to create protection systems that allow such tight control of digital works that the systems effectively grant new rights beyond the bounds of traditional copyright law."[84] The NGSCB platform, if the critics are correct, appears to have the possibility of fulfilling this prophesy of automated control in that it can enforce absolute restrictions on the user regardless of any limitations that exist within copyright law and regardless of whether the material is protected by copyright at all.

Some argue that the enforcement of copyright through the application of technology is not inconsistent with the doctrines of fair use and private copying. These legal pundits claim that these doctrines only exist because it was an area where copyright holders were not able to effectively control access and charge for the use of their works. Hence, when technology makes it possible to more completely control works then law should adapt and permit control.[85] Others, however, argue that the limitations to copyright are inherent in copyright itself—that it is the intention of the law to create a balance between the public and rights holders. Lessig states: ". . . my claim is simply that the law must be subject to the same limitations that a law protecting copyrighted material directly is."[86] It is this balance between access control and the value of having work in the public domain, and the legal underpinnings of this debate, that will be explored herein.

[84] Fallenböck, Ibid., p. 52.
[85] Lawrence Lessig, Ibid., p. 136.
[86] Lessig, Ibid., p. 188.

5.2 Copyright Protection

All of the major international instruments governing copyright provide for the granting of exclusive rights to creators of literary works for a limited period of time.[87] Among these rights is the most basic: the right to control reproduction.[88] However, this right is not all encompassing and is subject to the 3-step test first articulated in the Berne Convention. The test provides: 1)that exceptions to the exclusive right of reproduction are permitted in certain special cases, 2)provided that the reproduction does not conflict with the normal exploitation of the work, and 3)that such reproduction does not unreasonably prejudice the rights of the author.[89] Numerous limitations on an author's exclusive right to reproduction have developed. In the United States these limitations are encompassed in the fair use doctrine. Generally, within the European Union, copyright statutes provide an exhaustive list of limitations, but they generally allow for the same uses as are permitted under the fair use doctrine.

5.3 United States Approach

5.3.1 Fair Use Doctrine

The fair use doctrine provides for the use of copyrighted material in particular circumstances without first obtaining permission from the rights holder. In particular, the fair use doctrine supports: 1)private individuals making a limited number of copies of

[87] Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971, as amended on September 28, 1979, Article 7; World Intellectual Property Organization (WIPO) Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/94, Article 3; Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, World Trade Organization, Article 9.

[88] Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971, as amended on September 28, 1979, Article 9; World Intellectual Property Organization (WIPO) Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/94, Article 6; Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, World Trade Organization, Article 9.

[89] Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971, as amended on September 28, 1979,Article 9.

protected works for their personal use, 2)exceptions for educational uses of works, 3)criticism, and 4)research.

Unlike many civil law countries which provide an exhaustive list of uses that fall within a limitation on copyright, the United States Copyright Act[90] provides a four-step balancing test to assist in determining if a particular use falls within the fair use doctrine. The four step test examines: 1)the purpose and nature of the use including whether such use is for a commercial purpose or is for non-profit 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 or value of the copyrighted work.[91]

5.3.2 Constitutional Underpinnings of Fair Use

Within the United States, the debate over fair use inevitably leads to a discussion of the United States Constitution and the intent of the framers of the Constitution in drafting Article 8, Section 8, Clause 8. This provision of the Constitution provides authors with exclusive rights in their works for a limited period of time in order to promote progress. Many argue that the purpose of granting exclusive rights to copyright holders for a limited period of time is to provide them with an incentive to create works while also providing for these works to enter the public domain in the future.[92] Thus, in the context of fair use, some "…argue that copyright holders should receive only such incentives as are necessary to impel them to create and disseminate new works."[93] Hence, it is stated that copyright protection should only provide the level of protection

[90] 17 U. S. C. Section 107.
[91] Ibid.
[92] Jessica, Litman, "Revising Copyright Law for the Information Age", 75 Oregon Law Review 19 (1996), pp. 31-32.
[93] Ibid., p. 31-32.

necessary to create incentive and that everything beyond that which is necessary to promote the creation of new works should be left in the public domain. Lessig states: “The framers were as … concerned about establishing a constitutional requirement for an intellectual commons as they were about establishing a power to create intellectual property.”[94] Lessig’s view of the intent to have information in the public domain is hinted at by the United States Supreme Court in Feist Publications, Inc. v. Rural Tel. Serv. Co.[95]. In Feist, the Court states that facts and ideas are not protected by copyright, in part, because they should remain in the public domain where they “…may serve as building blocks for future authors and promote progress.”[96] In this sense, the fair use doctrine also provides a balance between copyright and the First Amendment right to free speech. However, in the DeCSS case, the court sought to limit the fair use doctrine in its statement that: “Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user’s preferred technique or in the format of the original.”[97] Burk and Cohen state: “Fair use partially reconciles these apparently contradictory constitutional provisions by allowing the use of otherwise protected material in criticism, comment, parody, news reporting, and similar uses in the public interest. This arrangement preserves proprietary rights in creative works while accommodating the public interest in open dialogue, deliberation, and the advance of knowledge.”[98] Interestingly, the case of Eric Eldred, et. al. v. John Ashcroft is currently

[94] Lawrence Lessig, ”The Limits of Copyright”, The Industry Standard, (June 19, 2000).

[95] 499 U. S. 340 (1991)

[96] Ibid., pp. 349-350.

[97] Universal City Studios, Inc. et al. v. Eric Corley, United States Court of Appeals for the Second Circuit, Docket No. 00-9185, Decided November 28, 2001, p. 17.

[98] Burk and Cohen, Ibid., p. 43 citing 17 U. S. C. Section 107 and Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985).

pending before the United States Supreme Court.[99] This case challenges the power of Congress to extend the copyright term and seems likely to require the Court to reconcile the balance between the First Amendment and Article 8, Section 8, Clause 8 of the United States Constitution.

Julie Cohen opines that "It follows that the law should not lightly allow copyright owners to opt out of the copyright framework of limited entitlements and into more robust entitlements of their own design."[100] Here the distinction is made between intellectual property and "traditional" forms of property. Because intellectual property rights are only granted for a limited period of time, the protection granted to the rights holder is something less than the protection of the owner of "traditional" property. Lessig states: "Intellectual property rights are a monopoly that the state gives to producers of intellectual property in exchange for their producing intellectual property. After a limited time, the product of their work becomes the publics to use as it wants."[101]

5.3.3 Technological Measures and Their Impact on Fair Use

One of the main impacts of technology on copyright exceptions such as the fair use doctrine is found in its ability to provide protection far greater than that provided for under copyright law. One example exists when a technological measure is used to control access to a work after the term for copyright protection has expired or where an access control measure is used to protect a work that is not sufficiently creative as to be protected by copyright law. Burk and Cohen state: "Rights management systems…can insist that permission be sought, and a fee paid, for any use. This is so…whether or not

[99] Eric Eldred, et. al. v. John Ashcroft, United States Supreme Court docket number 01-618.
[100] Burk and Cohen, Ibid., p. 43.
[101] Lessig, Ibid., p. 143.

the underlying information is still (or ever was) protected by copyright."[102] In this sense, it is argued that the technology itself becomes a form of law, especially when the technology itself is endorsed and enforced as it is under the DMCA anti-circumvention provisions. Burk and Cohen write: "If the integrity of the controls is backed by the state, as it is under the DMCA's anti-circumvention provisions, the legal enforcement of rights also shifts its focus from penalties for unauthorized infringement to penalties for access unauthorized by the rights holder."[103]

5.4 European Copyright

5.4.1 Limitations on Authors' Exclusive Rights

Like the United States, Member States of the European Union are also subject to the rules set forth in the Berne Convention, WIPO Copyright Treaty and the TRIPS Agreement. However, unlike the United States, the European Union opted to clearly delineate, in an exhaustive list, the circumstances in which an author's rights are subject to limitations. These limitations are set forth in Article 5 of the Copyright Directive. Much like the limitations under the U.S. fair use doctrine, the Directive permits Member States to limit the exclusive rights of an author for purposes of scientific research, quotation, criticism, parody, and a limited amount of private copying.[104] However, Burk and Cohen state: "…the E. U. Copyright Directive contemplates nothing so broad, flexible, or indeterminate as the U.S. concept of fair use. Rather, in the European

[102] Burk and Cohen, Ibid., p. 49.

[103] Ibid., p. 51.

[104] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

tradition of 'fair dealing,' the directive lists specific circumstances under which Member States may allow a user to make unauthorized use of a copyrighted work."[105]

5.4.2 Public Access Rights in the European Union

Unlike the United States, where both copyright and free speech (and to a lesser degree public access to information) are rooted in the Constitution, the European Union has no such document that sets forth a broad access right to information in the public domain. Such matters are typically left to regulation by individual Member States. However, it is worth considering the European Convention on Human Right in the context of access to information.

Article 10 of the European Convention on Human Rights provides: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[106] It is important to note, however, that such right to freedom of expression is limited to actions taken by the government and does not grant private individuals the right to demand access to information from rights holders or corporations. While no cases currently exist where an individual has demanded access to copyrighted material from another private actor, and brought action under Article 10, it seems doubtful that such a claim would succeed due to the limitations contained within the European Convention on Human Rights.

5.4.3 Technology's Impact on the Public Domain

The same concerns regarding the ability of technology to extend beyond the reach of copyright law exists in the European Union. However, in the European Union, the

[105] Burk and Cohen, Ibid., p. 70.

[106] European Convention on Human Rights and its Five Protocols, (Rome 4 November 1950, as amended in Strasbourg 20 January 1966), Article 10.

Copyright Directive appears to offer better remedies for a user who has his or her rights excessively limited by an overreaching technological measure. As discussed in Chapter 3, Article 6(4) of the Copyright Directive, permits Member States to take steps to ensure that the limitations on copyright are not eroded by the application of technological measures. However, as noted in Chapter 3, implementation in Member States of Article 6(4) is highly varied.

5.5 Summation of Chapter 5

Currently, while both the United States and the European Union have delineated exceptions to an author's exclusive rights under copyright, technological measures and the protection of these measures through prohibitions against circumvention threaten to upset the balance that has traditionally existed. Lessig argues that the balance between rights holders and the public is necessary in order to create an "intellectual commons".[107] The intellectual commons is a place where ideas, works, and information are shared in the public domain free from control and interference by others. However, the continued privatization of intellectual property through the legal support of access and copy controls threatens the continuation of the "intellectual commons". The next chapter will explore the ways in which the digital technology that imposes restrictions on access and control can be modified to preserve the limitations to copyright while still enabling rights holders to adequately protect themselves against piracy.

[107] Lessig, Ibid., p. 143.

Chapter 6: Proposed Solutions for Preserving the Balance

6.1 Introductory Comments

Currently the provisions contained in both the DMCA and the Copyright Directive prohibiting both the act of circumvention and the trafficking in circumvention devices threatens to extinguish copyright limitations. Where, in recent times, we have seen the rule of law change to support the technologies employed by rights holders to protect their works, the same rule of law can, and should, now be applied to protect the public domain. If underlying changes in the way systems are designed are reinforced through the rule of law, the balance between the needs of rights holders and the public can be preserved. In this sense, the combination of law and technology could be applied to mirror the manner in which copyright law operates in relation to non-digitized products in the off-line world. The proposed options for preserving fair use in the digital age were first set forth in an article by Dan L. Burk and Julie E. Cohen entitled "Fair Use Infrastructure for Digital Rights Management Systems." The possibility of implementing both the architecture changes and legal changes is explored herein. Finally, the application of these proposed changes in the context of the NGSCB project will be considered.

6.2 Changes in Systems Architecture

Burk and Cohen state: "The most direct method of accommodating fair use would be to mandate or prompt the development of rights management systems that directly allow purchasers of a work to make fair use of the content."[108] This suggests that the underlying computer code could be developed in a manner that would support and

[108] Burk and Cohen, Ibid., p. 55.

enforce the limitations that exist within copyright. In relation to the fair use doctrine, they suggest that the system architecture could be altered to allow small portions of a work to be accessed a certain number of times without paying additional fees and without the permission of the rights holder.

A central challenge to altering the system architecture to accommodate the fair use doctrine in the United States exists in that the parameters of the doctrine are determined through the application of the four-part balancing test. Burk and Cohen note that: "Building the range of possible uses and outcomes into computer code would require both a bewildering degree of complexity and an impossible level of prescience."[109] It is noted that while the application of the fair use doctrine is dynamic, system architecture is static. Anticipating the range of possible applications of the fair use doctrine would be an impossible task for system designers. Furthermore, the amount of digitized content that can be accessed and still fall within fair use changes depending on the context in which the use is made.

It is important to note that building in a range of possible actions that accommodate the limitations found in the Copyright Directive Article 5 would not be as challenging a task as under U.S. law since Article 5 more clearly delineates copyright limitations. However, even in the European Union, translating the delineated limitations to copyright into computer code would prove a daunting task.

Given the complexity of trying to translate all copyright limitations into computer code, Burk and Cohen suggest that system architecture be altered so that uses that most commonly fall within fair use are accommodated through the new architecture and without having to obtain permission from the rights holder. As opposed to establishing a

[109] Ibid., p. 56.

bare minimum of permitted fair uses, it is suggested that standards be established by examining the "…daily behavior of ordinary users."[110] Burk and Cohen state: "Rather than approximating the results of fair use jurisprudence or the products of interest-group bargaining, rights management systems might be designed to approximate fair use norms."[111] Under this proposed solution, it is acknowledged that there would likely be both widespread unauthorized copying of a small quantity and that certain uses that are actually permitted by copyright law would not be accommodated. Because of the challenges posed by requiring computer code to be changed to accommodate fair use, it is necessary to explore other means of preserving the public's access to information.

6.3 Key Escrow System

The key escrow system of enforcing the limitations of copyright would involve having a third party make and impose decisions about whether a proposed use falls within an established copyright limitation. However, this proposal has numerous drawbacks. Specifically, the use of a third party to make fair use determinations on a case by case basis is extraordinarily costly and time consuming. Moreover, having to apply to a third party for permission in advance affects an individual's ability to use works or portions thereof spontaneously. Lastly, the involvement of a third party harms an individual's ability to use works anonymously. It is important to remember that prior to the introduction of technological measures for enforcement of access and copying controls, an individual could make use of works however they wished subject only to being held liable for damages if such use constituted an infringement.

[110] Ibid., p. 57.
[111] Ibid., p. 58.

Given these drawbacks, Burk and Cohen have suggested a modified version of a key escrow system where the keys are held by a trusted third party.[112] Under their proposal the trusted third party would be given the cryptographic keys by rights holders. It is suggested that the trusted third party be a publicly funded institution so that users would not be required to pay fees for access. The third party would release the keys to those seeking to exercise their fair use rights. Rather than enter into a detailed analysis of whether a particular use is within an established copyright limitation, the trusted third party would simply release the keys and keep a record of the transaction. To help overcome some of the privacy issues, the user's record would only be released upon court order and based on a finding of actual infringement.[113] It is important to note that this system still has an impact on the individual's ability to use works spontaneously and may still have a "chilling effect" as privacy is not absolutely protected.

6.4 Combining System Architecture and Key Escrow to Preserve Fair Use

Because neither a system of altering the underlying system architecture nor the key escrow system on its own can achieve the desired results of preserving copyright limitations, Burk and Cohen suggest designing a dual infrastructure based on combining both proposed solutions. It is suggested that a law be implemented requiring rights management systems to incorporate the most common copyright limitations into the system architecture. Such a system should automatically include fair use that is "…based on customary norms of personal noncommercial use."[114] For uses that are within a copyright exception, but beyond what has been included in the system architecture, the user would obtain access from a trusted third party.

[112] Ibid., p. 64.
[113] Ibid.
[114] Ibid., p. 65.

The success of the proposed system relies on changes to the existing copyright laws. In order to obtain participation in such a system by rights holders, it is suggested that the copyright law could condition enforcement on meeting the required level of access for system architecture. Moreover, the anti-circumvention provisions of both the DMCA and the Copyright Directive would have to be altered. It is proposed that the circumvention provisions would remain intact and would apply for users who fail to access works via the trusted third party. However, for rights holders who elect not to deposit cryptographic keys with the trusted third party, it is suggested that the anti-circumvention provisions would not apply. Burk and Cohen state: "For such unescrowed works, a 'right to hack' would effectively substitute for access via the escrowed keys. As noted … the ban on the manufacture and distribution of circumvention technologies would need to be modified to make this defense a realistic possibility."[115]

6.5 Required Modifications Under the DMCA and The Copyright Directive

In order for this proposed solution to be implemented, changes would need to be made to both the DMCA and the Software Directive. Under the DMCA Section 1201 changes would need to be implemented to all three anti-circumvention provisions. First, Section 1201(a)(1)(a) would need to be amended to incorporate new rules allowing access circumvention if the rights holder elects not to place the cryptographic keys into the key escrow. The criterion related to determining the "effectiveness" of a particular technological measure should remain intact, as it should still be applied in circumstances where a user elects to circumvent a technological measure despite the rights holder having placed the keys in escrow. Secondly, both provisions relating to the trafficking of

[115] Ibid., p. 66.

anti-circumvention devices (Sections 1201(a)(2) and 1201(b)) will need to be amended to permit the sale and distribution of circumvention technology. Here, if circumvention technology was used to gain access to a work where the keys were not placed in escrow, the rights holder would not be permitted to hold the user liable under the trafficking provisions. In the situation described above, the user would have to be exempted from criminal liability as well. Perhaps more importantly, the DMCA would have to be altered to create a proactive requirement that systems engineers be required to provide minimal fair use functionality during the process of creating digital rights management systems or "trusted systems". As discussed above, the minimum level should comply with customary noncommercial use.

As with the DMCA, the Copyright Directive would have to be modified to permit the creation of a key escrow system. The Copyright Directive Article 6(1) would need to be modified to permit the act of circumvention where the rights holder had not deposited the cryptographic keys into the key escrow. Moreover, Article 6(2) would need to be modified to permit the trafficking in circumvention devices. As with the DMCA, a new provision requiring a minimal level of fair use to be incorporated in the system architecture of digital rights management systems.

6.6 Compliance with International Treaty Obligations

In order for a system architecture/key escrow system for preserving the balance in copyright law to be viable it must comply with all international treaty obligations. Specifically, this proposed solution must comply with the requirements of the WIPO Copyright Treaty, the Berne Convention and the TRIPS Agreement.

As the WIPO Copyright Treaty is the only international instrument requiring the enforcement of technological measures, it is of most concern in considering the implementation of the proposed system architecture/key escrow system. As discussed in Chapter 3, the WIPO provisions relating to the protection of technological measures are contained in Article 11. Clearly, it is necessary to determine whether the proposed amendments to both the DMCA and the Copyright Directive will violate Article 11. However, it is important to remember that both the DMCA and the Copyright Directive have implemented Article 11 in a manner that exceeds the scope required in the WIPO Copyright Treaty. As the WIPO Copyright Treaty incorporates the copyright limitations contained in the Berne Convention, it clearly recognizes and preserves the fair use limitation. The only portion of Article 11 that poses a potential problem is the wording restricting acts ". . .which are not authorized by the authors concerned…."[116] One could argue, however, that since the treaty recognizes the exceptions set forth in the Berne Convention, that it is not with the prevue of rights holders to "authorize" an action that is already permitted under the law. Even if modification of the WIPO Copyright Treaty is required, the amendment to Article 11 would be minor and could be accomplished simply by removing the reference to actions approved by rights holders since Article 11 already applies to actions that are not permitted by law.

With respect to the Berne Convention, Article 5(2) is of most concern in implementing the system architecture/key escrow proposal. Article 5(2) provides that the ". . .enjoyment and the exercise of (copyright) shall not be subject to any formality."[117] However, it can be argued that the proposed system architecture/key escrow solution

[116] WIPO Copyright Treaty, Ibid., Article 11.

[117] Burk and Cohen, Ibid., p. 72.

does not violate Article 5(2) as it ". . . affects remedies rather than rights…."[118] The proposed solution does not alter the underlying copyright protection afforded to rights holders under the Berne Convention. As the TRIPS Agreement incorporates the Berne Convention, no additional issues are raised under the Agreement.

6.7 Modification for NGSCB Compliance

In order for the NGSCB technology to comply with the proposed legal changes suggested here, several modifications would need to be incorporated into the NGSCB technology. Two central changes need to be made to ensure that a balance between the interests of rights holders and those of the public are preserved in copyright law.

First, Microsoft would need to ensure that the users of the NGSCB technology have access to the cryptographic key pairs. It is imperative that users have access to the cryptographic keys in order to comply with the key escrow system presented above and to prevent the unauthorized remote deletion of the content on their computers. Moreover, Microsoft needs provide users with access to works created by the user even if the license for the software that was used to create the work has expired or been revoked. Here, it would be acceptable for read-only access to be provided. Microsoft, by controlling the NGSCB operating system, also has the power to control the dissemination of derivative works if access to software is denied and the cryptographic key pairs are not released to the user. Allowing a single corporation to hold the cryptographic keys not only places the entity in a position to control the distribution of derivative works, but is also contrary to the principles of democracy. Democracy requires a separation of power between the creators of laws (i.e. legislatures or parliaments) and those charged with the interpretation and enforcement of laws (i.e. the judicial system). By permitting Microsoft to hold the

[118] Ibid.

cryptographic keys and to determine the circumstances in which content can be removed, does not comply with the core principles of democracy.

Finally, Microsoft should alter NGSCB's architecture to ensure that only access to protected content can be controlled. The current state of the technology will enable material that does not meet the standards for copyright protection to be controlled using NGSCB. It seems likely that Microsoft will have little incentive to incorporate this change into NGSCB's architecture unless it is required by law, or unless the legal regime endorses a "right to hack" if keys are not deposited in escrow. The creation of a "right to hack" if the cryptographic keys are not deposited in the key escrow creates a large incentive for compliance by Microsoft as they will wish to preserve the integrity of the NGSCB system and source code that they have invested in creating.

Chapter 7: Conclusion

In recent years, primarily fueled by the increase in distribution of digital materials via the Internet, we have seen a movement by rights holders to seek out means to better protect their works from piracy. The solution was found through the use of technology aimed at providing better control over digitally distributed products. However, the increase in the use of technology to control works has also resulted in a dramatic change in the balance that has traditionally existed in copyright law. Moreover, legal rules and regulations have expanded to not only protect rights holders under copyright law, but also, to protect the technologies employed by rights holders.

The use of technology to protect works and the endorsement of such technologies by law has had several far reaching effects. First, there has been a shift from protecting copyright in works to controlling and regulating access to works. This shift to access control also applies to works for which the copyright has expired or never existed. This has prevented works from entering the public domain. Moreover, the move to control access to works, whether protected by copyright or not, has resulted in a divergence in the level of protection offered for digital products and for products distributed by more traditional means.

The shift to protection through the use of technology has also led to an increased privatization of law that results in a loss of transparency. By permitting copyright decisions to be made by rights holders in secret often leaves users without fast and affordable access to the courts and often without notice of the actions taken against them. Most harmful, however, is that it is not necessary a legal application of copyright law, but rather the rights holders view of copyright law that prevails. Lessig writes: "Just as we don't privatize every public park, every street, and every idea, we can't privatize every feature of cyberspace."[119]

It appears, however, that these technological advances will continue to challenge our traditional notions of copyright especially within the context of fair use. Many predict that in the coming years the Internet will lose its character as open intellectual space. If technologies, like NGSCB, continue development with the endorsement of the legal regime, much of the openness of the "intellectual commons" that currently exists will be lost. Hugenholtz concludes: "In the end, only a new body of information law, replacing traditional copyright law, will be able to save the diminishing public domain."[120]

[119] Lessig, Lawrence, "Open Code and Open Societies: Values of Internet Governance", 74 Chicago Kent Law Review, 1405 (1999), p. 1420.

[120] Hugenholtz, Ibid., p. 318.

Clearly, without government intervention, the balance and transparency that has traditionally existed within copyright law will be lost. With the endorsement and protection of technological measures, the balance that was traditionally found within copyright law has already been distorted and unless the law intervenes to restore the balance, the "intellectual commons" will disappear. However, as discussed herein, the balance can be restored through a combination of changes to existing law, through technological engineering, and through the development of a key escrow system.

With respect to the NGSCB project, it is evident that some changes ought to be incorporated prior to the release of the NGSCB technology. The central issue with NGSCB appears to center around the user not having access to the cryptographic keys. A user should have the ability to determine who shall hold the cryptographic keys to his or her system. Additionally, as was suggested in the preceding chapter, the NGSCB technology should implement underlying system architecture changes to ensure that the application of NGSCB as a digital rights management system comports with fair use social norms. However, without legislation requiring these changes, Microsoft seems unlikely to implement them since the major distributors of digital content form a valuable market for the NGSCB product, as well as a powerful lobby within the United States. Increasingly, actors within the fields of digital technology and content distribution will choose to "opt out" of the legal system that protects copyright. Without the implementation of changes to the current regulatory regime, it seems only a matter of time, before the technology that the legal regime has endorsed, makes the courts and laws increasingly irrelevant.

References

List of Judgments/Decisions

Feist Publications, Inc. v. Rural Tel. Serv. Co. 499 U. S. 340 (1991).

Universal City Studios, Inc. et. al. v. Eric Corley, United States Court of Appeals for the Second Circuit, Docket No. 00-9185, Decided November 28, 2001.

Universal City Studios, Inc. v. Reimerdes, et al., 111 F. Supp 2d 346 (S.D.N.Y. 2000).

Treaties

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), World Trade Organization.

Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971, as amended on September 28, 1979.

European Convention on Human Rights and its Five Protocols, Rome 4 November 1950, as amended in Strasbourg 20 January 1966.

World Intellectual Property Organization (WIPO) Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/94.

World Intellectual Property Organization (WIPO) Performances and Phonograms Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/95.

Statutes

United States Constitution, Article 8, Section 8, Clause 8.

Digital Millennium Copyright Act, enacted October 20, 1998, Title 17 United States Code.

Directives

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce).

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

Secondary Literature

Anderson, Ross, "TCPA/Palladium FAQ's", www.epic.org.

Biegel, Stuart, Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace, (Cambridge, Massachusetts: The MIT Press, 2001).

Boutin, Peter, "Palladium: Safe or Security Flaw", Wired News, www.wired.com/news/antitrust/0,1551,53805,00html.

Burk, Dan L. and Julie E. Cohen, "Fair Use Infrastructure for Rights Management Systems", Harvard Journal of Law and Technology, Volume 15, Number 1 (Fall 2001).

Clark, C., "The answer to the machine is in the machine", The Future of Copyright in a Digital Environment (P. Bernt Hugenholtz, ed., 1996).

Gates, Bill, Executive Email, "Trustworthy Computing", July 18, 2002. www.microsoft.com/mscorp/execmail/2002/07-18twc-print.asp.

Cringely, Robert X., "I Told You So: Alas, a Couple of Bob's Dire Predictions Have Come True", I, Cringely, The Pulpit, www.pbs.org/cringely/pulpit/pulpit20020627.html.

Fallenböck, Markus, "On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions", International Journal of Communications Law and Policy, Issue 7 (Winter 2002/2003).

Hugenholtz, Bernt P., "Code as Code, Or the End of Intellectual Property as We Know It", 6 MJ 3 (1999).

Huppertz, Marie-Thérèse, "The Pivotal Role of Digital Rights Management Systems in the Digital World—An analysis of the copyright protection provided for in the 2001 Copyright Directive with a specific emphasis on the protection of the digital rights management systems and their implementation into the national law", Cri 4/2002.

Julià-Barceló, Rosa, "Section 4: Intermediaries: Ch. 1: Liability for on-line Intermediaries: Comparing EU and US Legal Frameworks," (Walden, Ian & Hörnle, Julia, editors, Woodhead Publishing Limited 2001).

Lemos, Robert, “Trust or Treachery? Security Technologies Could Backfire Against Consumers”, CNETnews (November 7, 2002), http://news.com.com/2009-1001-964628.html.

Lessig, Lawrence, Code and Other Laws of Cyberspace, (New York: Basic Books, 1999).

Lessig, Lawrence, “The Limits of Copyright”, The Industry Standard, (June 19, 2000).

Lessig, Lawrence, The Future of Ideas: The Fate of the Commons in a Connected World, (New York: Vintage Books, 2002).

Lessig, Lawrence, ”Open Code and Open Societies: Values of Internet Governance”, 74 Chicago Kent Law Review, 1405 (1999).

Litman, Jessica, “Revising Copyright Law for the Information Age”, 75 Oregon Law Review 19 (1996).

Microsoft Next-Generation Secure Computing Base – Technical FAQ, (January 12, 2002), www.microsoft.com/technet/security/news/NGSCB.asp?frame=true.

Microsoft Press Pass, Microsoft “Palladium”: A Business Overview, (June 18, 2003), www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp.

Report of the Senate Committee on the Judiciary, S. Rep. No. 105-190, (1998).

Schoen, Seth, “Palladium Details”, ActiveWin, (July 8, 2002), www.activewin.com/articles/2002.pd.html.

Stallman, Richard, “Can You Trust Your Computer?”, News Forge: The Online Newspaper of Record for Linux and Open Source, (October 21, 2002), www.newsforge.com/newsforge/o2/10/21/1449250.shtml?tid=9.

TCPA Frequently Asked Questions, Rev. 5.0, (July 3, 2002), www.tcpa.org.

Thornburg, Elizabeth, “Going Private: Technology, Due Process, and Internet Dispute Resolution”, 34 U.C. Davis Journal of International Law and Policy 151 (2000).

Patents

Patent No. 6,330,670, http://www.patft.uspto.gov/netahtml/srchnum.html.

Patent No. 6,327,652, http://www.patft.uspto.gov/netahtml/srchnum.html.