Locking Down Loose Bits:
Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer

by Ryan Roemer

Locking Down Loose Bits - Table of Contents:

"The end result will be failure. All digital copy protection schemes can be broken, and once they are, the breaks will be distributed ... law or no law. ... Digital files cannot be made uncopyable, any more than water can be made not wet. "

- Bruce Schneier, cryptography expert [1]

Introduction

Digital copy protection is emerging as one of the highest stakes issues for consumer rights, digital age business models, and copyright law. To date, content owners have been on the losing end of a battle over bits. Hackers have successfully cracked copy protection on everything from DVD's to copy-proof CD's. Conscious of the failure of digital content protection systems and the widespread distribution of unauthorized copyrighted works over the Internet, the content industry is desperate for a technological or legal content protection. Most eyes are currently turned to advances in "digital rights management" ("DRM") technologies, which offer an unprecedented level of control over digital content. Additionally, such control could create new, restrictive business models and revenue sources for the content industry.

At the same time, the technology industry has been quietly developing an initiative known as "trusted computing," which aims to put security features deep into the hardware of personal computers. Trusted computing systems can protect individual files and sensitive data on a computer, as well as verify that the components of a computer are

---

* Ryan Roemer received his J.D. from the UCLA School of Law in 2003. He would like to thank Prof. Stuart Biegel for his guidance and support in the research and writing of this paper.

[1] Bruce Schneier, *The Futility of Digital Copy Prevention*, Crypto-Gram Newsletter, May 15, 2001, *at* http://www.schneier.com/crypto-gram-0105.html#3 (last visited Dec. 26, 2003) [hereinafter Schneier, *The Futility of Digital Copy Prevention*]. Schneier is the CTO and founder of Counterpane Internet Security and inventor of the Blowfish encryption algorithm.

in a known state.[2] Such a technology poses great advantages for electronic commerce as well as personal security for the public.[3]

At the intersection of digital rights management and trusted computing lies a new approach to content protection. The content industry is pressing the technology industry to utilize the security of trusted systems to enable a much stronger digital rights management scheme. Many academics and civil libertarians worry that absolute content control could cause collateral damage. Advancing digital rights management technology could render many public freedoms under copyright law technologically impossible, while expanding liability under the controversial Digital Millennium Copyright Act.

This paper will examine the copyright implications of the new trusted computing initiative as a building block for stronger digital rights management schemes. As with many emerging technologies, there is some debate as to what "trusted computing" actually describes. In the academic and civil libertarian circles, "trusted systems" and "trusted computing" are often synonymous with digital rights management.[4] Moreover,

---

[2] David Safford, *The Need for TCPA*, IBM Watson Research - Global Security Analysis Lab (Oct., 2002), *available at* http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf [hereinafter Safford, *The Need for TCPA*].

[3] *Id*. ("Hackers on the internet present a threat to clients and to the authentication used in electronic commerce applications. Our client side operating systems and application are so complex, that bugs and security vulnerabilities in software are virtually inevitable. It is therefore critical to provide some hardware base protection for sensitive authentication and encryption keys, that protects them from hackers even in the presence of vulnerable software. TCPA provides this critical hardware security function, protecting an individual's authentication and encryption keys from remote software attack.").

[4] Mark Stefik, a scientist at Xerox's renowned Palo Alto Research Center was one of the first commentators to postulate the possibility of "trusted systems" as applied to digital rights management. *See, e.g.,* Mark Stefik, *Shifting The Possible: How Trusted Systems And Digital Property Rights Challenge Us To Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137 (1997). Many academic observers have lifted the "trusted system" terminology to encompass all system-wide DRM approaches. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 127 (Basic Books 1999) (referencing Stefik) [hereinafter Lessig, CODE]; Elizabeth G. Thornburg, *Going Private: Technology, Due Process, and Internet Dispute Resolution*, 34 U.C. Davis L. Rev. 151 (Fall, 2000) [hereinafter Thornburg, *Going Private*]. Open source software advocates similarly assume that the technological trusted computing technologies will be used for digital rights management restrictions. *See, e.g.*, Eben Moglen, *Untrustworthy Computing*, Free Software

even knowledgeable critics within the technology community often "improperly lump together TCPA [the Trusted Computing Platform Alliance specification], Palladium, and DRM, considering them as one thing."[5] To these commentators, "trusted systems" are a tool that absolutely enforces copyright restrictions and prevents digital copyright infringement on an end user's computer.

However, the actual technology dubbed "trusted systems" and "trusted computers" presently under development doesn't quite fit this bill. Technological "trusted systems," as touted by the Trusted Computing Group and Microsoft's Next Generation Secure Base, will not restrict digital content, nor implement *any* digital rights management scheme. Technological trusted systems are only security sub-systems, available for any number of security purposes. Consequently, this paper will use the phrases "trusted computing" and "trusted systems" to describe emerging trusted technologies, and not the academic / civil libertarian general concept of digital rights management.

This paper contends that advent of trusted computing has serious implications for the evolving digital copyright debate. First, digital rights systems based on trusted

---

Matters (August 2002), *available at* http://emoglen.law.columbia.edu/publications/lu-22.html; Richard Stallman, *Can You Trust Your Computer?*, GNU Project, *at* http://www.gnu.org/philosophy/can-you-trust.html (last visited Dec. 17, 2003) (referring to the trusted computing initiative as "treacherous computing") [hereinafter Stallman, *Can You Trust Your Computer?*].

[5] David Safford, *Clarifying Misinformation on TCPA*, IBM Watson Research - Global Security Analysis Lab (Oct., 2002), *available at* http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf [hereinafter Safford, *Clarifying Misinformation on TCPA*]. Safford is in the particularly credible position of having already developed and released TCPA-compliant trusted computing technologies. Safford points out many technical inaccuracies in criticisms by Ross Anderson (referenced *infra*), Lucky Green and Bill Arbaugh. His article rebukes such fears as trusted computing won't run on open source platforms such as Linux by noting that "the fact is that we are working on releasing TCPA code for Linux under the GPL." *Id*. IBM made good on Safford's claim by releasing TCPA software for Linux under the GNU General Public License, currently *available at* http://www.research.ibm.com/gsal/tcpa/tpm-1.1.tar.gz (software in archived format, not a web page).

computing technology will create additional complications for anti-circumvention liability under the Digital Millennium Copyright Act. Second, trusted computing and digital rights management could effectively "privatize" copyright law - enabling content owners, and not the law, to decide exactly what rights the public will have over digital content. Finally, trusted computing cannot completely secure digital rights management over the long term. In fact, this paper will argue that no technology can. The content industry's continuing legal and technological pursuit of digital rights management in the face of technological impossibility threatens to create a digital "arms race," harming the balance of copyright law and consumer rights.

Part I of this paper explores digital rights management, both as a possible cure for digital piracy and as a tool for absolute control of copyrighted works. Part II explores the rapidly developing field of trusted computing, and follows the two most prevalent initiatives - the Trusted Computing Group and Microsoft's Next Generation Secure Computing Base. Part III contends that despite the security advances of trusted computing, no technology can enforce perfect digital rights management. Part IV gives a brief background of traditional copyright law and specifically examines liability for the circumvention of technological protection measures under the Digital Millennium Copyright Act and the DeCSS case. Part V examines the legal and technological intersection of copyright law and digital management, as trusted computing quickly becomes a tangible reality.

I. The Present State of Digital Rights Management

A. Introduction to Digital Rights Management

"Digital Rights Management" ("DRM")[6] generally describes technologies that "restrict the use of digital files in order to protect the interests of copyright holders."[7] DRM can prevent or restrict a computer[8] from "altering, sharing, copying, printing, [or] saving" protected digital files.[9] More importantly, DRM allows copyright owners very detailed control over the ways in which a user may access their files (how long they may view a file, how many times a file may be accessed, etc.).[10] By way of example, Disney could release a digital video file of "Snow White" to a fictional user, Joe, that could only be played on the Joe's personal computer ("PC"), could not be copied or altered, and could be watched only 3 times.[11] After watching the video twice, Joe could not loan his file to a friend to use up his third viewing, as it only plays on Joe's specific computer. If Joe wanted to watch the video file more than 3 times, or wished to save a portion of the video for his own personal use, he would be unable to do so without further permission from Disney.

---

[6] "DRM" is the most popular variation within a large pool of synonymous phrases and acronyms. For a description of various alternative terms, *see* Electronic Privacy Information Center, *Digital Rights Management and Privacy*, *at* http://www.epic.org/privacy/drm (last visited Dec. 17, 2003) ("DRM may also be referred to as 'Content Management Systems' (CMS), 'Content/Copy Protection for Removable Media' (CPRM) or sometimes as 'technological measures.'") [hereinafter EPIC, *Digital Rights Management and Privacy*].

[7] *Id*.

[8] I use the "computer" to include the wide range of electronic devices that can utilize digital files, including embedded systems, mp3 players, personal digital assistants ("PDA's"). For example, *see* LinuxDevices.com, *Embedded Linux gets Digital Rights Management support*, LinuxDevices.com, Jan. 9, 2003 (noting Macrovision's Macrosafe software for "a variety of non-PC devices including set-top boxes, PDAs, portable entertainment devices, and digital consumer electronics appliances, in addition to traditional PCs"), *at* http://www.linuxdevices.com/news/NS4835727996.html.

[9] EPIC, *Digital Rights Management and Privacy*, *supra* note 6.

[10] *See id*.

[11] Example adapted from Ross Anderson, *TCPA / Palladium Frequently Asked Questions*, *at* http://www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html (last visited Dec. 17, 2003) [hereinafter Anderson, *TCPA / Palladium FAQ*].

DRM relies on two primary aspects to secure content for digital rights owners: "containment" and "marking."[12] The content industry's concern is that once a digital file is sent to the user's computer, the user may attack and extract the information from the file for unrestricted use. Thus, for DRM to work, the digital content must be "contained" so that it may only be accessed in authorized ways.[13] "Containment" is generally accomplished by encrypting distributed digital content so that only programs authorized by rights owners may decrypt, and thus access the information.[14] Additionally, DRM systems must "mark" which uses of a digital file are authorized.[15] This may be done with a "watermark," "flag" or an XrML[16] tag.[17] Returning to the previous example, Joe's digital video file of Snow White could be encrypted ("contained") so that Joe would be unable to access the data by any means other than a Disney-approved viewing program. Joe's video file would be "marked" in XrML with the instructions to: (1) play only on Joe's computer, (2) disallow any copying or alteration, and (3) play only 3 times. The video program would understand these instructions and limit Joe's viewing of Snow White accordingly.

---

[12] EPIC, *Digital Rights Management and Privacy*, *supra* note 6.
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] "XrML" is the abbreviation for "eXtensible Rights Markup Language," which provides a common syntax for DRM rules. *See XrML Frequently Asked Questions*, *at* http://www.xrml.org/faq.asp (last visited Mar. 12, 2003) ("The eXtensible rights Markup Language™ (XrML™) is a general-purpose, XML-based specification grammar for expressing rights and conditions associated with digital content, services, or any digital resource."). This allows technology developers to create programs and frameworks which uniformly understand and adhere to a common "language" of what digital access to provide for end users in their DRM products. *See id*. ("XrML, as a language for specifying rights and conditions, is a core component of a digital rights management system (DRM). It expands the capabilities of the DRM system and brings to it features often missing in proprietary implementations. If you already have a DRM system in place, then the DRM system would have to be modified to take advantage of XrML.").
[17] EPIC, *Digital Rights Management and Privacy*, *supra* note 6.

B. The Inherent Insecurity of Bits

Existing DRM systems are susceptible to attacks or reverse engineering that render digital content unprotected. Presently, digital content must be downloaded or streamed to an end user's computer. Once that information resides on an end user's computer, it is particularly vulnerable. Professor Ed Felten of Princeton University contends that both the "containment" and "marking" DRM techniques can be defeated by end users with even "moderate" programming skills.[18]

Ed Felten classifies two "threat" models for digital content owners.[19] The first is the "Napsterization" threat model, which "assumes that there are many people, some of them technically skilled, who want to redistribute [a copyrighted] work via peer-to-peer networks; and it assumes further that once [the digital] content appears on a p2p network, there is no stopping these people from infringing."[20] Security under the Napsterization model must ultimately prevent even *one* copy of a digital file from breaking the security of the DRM system, because one copy may be widely distributed and used over the Internet. This threat model requires that a "DRM technology must be strong enough to stymie even the most clever and determined adversary."[21]

The second threat model is the "casual-copying" model, which "assumes that you are worried about widespread, but small-scale and unorganized, copying among small groups of ordinary consumers."[22] The casual-copying model isn't concerned with *de minimis* digital file cracks, provided that the majority of distributed copyrighted files

---

[18] *Id* (quoting Professor Ed Felten).
[19] Ed Felten, *DRM, and the First Rule of Security Analysis*, Freedom To Tinker (Mar. 19, 2003), *at* http://www.freedom-to-tinker.com/archives/000317.html [hereinafter Felten, *DRM, and the First Rule of Security Analysis*].
[20] *Id*.
[21] *Id*.
[22] *Id*.

remain secure. Securing against a casual copying threat model is a much more feasible goal for DRM systems.

Professor Felten notes that most digital content owners complain about the Napsterization model, while proposing DRM solutions that address the casual-copying threat model.[23] However, solving the Napsterization threat model would require a DRM system to prevent single attacks from threatening the entire system. Peter Biddle et al., of Microsoft Corporation, notes that such a DRM system must "strive to be BOBE (break-once, break everywhere)-resistant."[24] Biddle concludes that the ultimate goal in DRM design is to create a situation where "knowledge gained breaking one client cannot be applied elsewhere."[25]

The growing concern is that a BOBE-resistant DRM system, capable of defeating the Napsterization threat model, may well be impossible. The emerging consensus among security experts is that DRM is "fundamentally insecure."[26] Ed Felten observes that although theoretically unbreakable encryption codes exist, DRM systems cannot utilize these effectively to secure their content .[27] DRM systems must ultimately leave digital content on the computer of an end user, a "presumed adversary," who has any length of time to attack a DRM file.[28] Moreover, digital content must eventually be

---

[23] *Id*.
[24] Peter Biddle et al., *The Darknet and the Future of Content Distribution* (Oct. 15, 2002), *available at* http://crypto.stanford.edu/DRM2002/darknet5.doc.
[25] *Id*.
[26] Ed Felten, *Why Unbreakable Codes Don't Make Unbreakable DRM*, Freedom To Tinker (Dec. 3, 2002) ("It's commonly understood among independent security experts that DRM (i.e., copy prevention) technology is fundamentally insecure, at least based on today's state of the art."), *at* http://www.freedom-to-tinker.com/archives/000214.html [hereinafter Felten, *Why Unbreakable Codes Don't Make Unbreakable DRM*].
[27] *Id*. ("unbreakable codes, whether theoretically impregnable or practically untouchable, do not imply that DRM is possible.").
[28] *Id*.

decrypted into a usable format (sound, video, etc) by an authorized DRM program, creating another opportunity for interception and attack.

Abstractly, the hopes for secure DRM are bleak. In practice, the situation is much worse. To date, most DRM systems have been circumvented with trivial effort. In September, 2000, the Secure Digital Music Initiative ("SDMI") opened up a public contest to see if any developers could break its DRM watermarking scheme for digital music files.[29] Theoretically, this "watermark" would prevent any unauthorized use or illicit copying, because the music file would be unplayable under unauthorized circumstances.[30] By November 2000, Professor Ed Felten and a group at Princeton University successfully broke the entire scheme. Their attack removed the watermark and converted the digital file into an unprotected format without degrading the music quality of the file.[31] Consequently, a single DRM-protected file released in SDMI format can be (1) cracked, so that an end user can play the file in an unauthorized manner, (2) cracked using techniques that should work on *any* SDMI file, and (3) ultimately released to the public at large in the popular (and unprotected) MP3[32] format, thwarting all existing SDMI protection for that specific music file. Professor Felten postulates that the experience with SDMI is indicative of a greater problem with current DRM technologies: "The underlying problem that SDMI is trying to solve, that of protecting content from a

---

[29] *See* Secure Digital Music Initiative, *SDMI Opens Public Challenge* (Sept. 18, 2000), *available at* http://www.sdmi.org/pr/BR_Sept_18_2000_PR.htm.

[30] *See* Ed Felten et al., *SDMI challenge FAQ*, *at* http://www.cs.princeton.edu/sip/sdmi/faq.html (last visited Dec. 17, 2003) ("A digital watermark is an imperceptible signal hidden in an audio clip, or an image, or any other object of value. The hidden signal is intended to communicate information about the marked object. ... In the context of SDMI, the application is screening and piracy prevention: an audio clip with a watermark is recognized as copyrighted, warning a portable device that it should not be recorded (or possibly even played) except under specific conditions.") [hereinafter Felten, *SDMI challenge FAQ*].

[31] *See* Ed Felten, *Status of the paper "Reading Between the Lines: Lessons from the SDMI Challenge"*, *at* http://www.cs.princeton.edu/sip/sdmi/ (last visited Dec. 17, 2003) (providing details and links to the Princeton group's successful attack on the SDMI scheme and subsequent threatened legal action under the DMCA by the RIAA and SDMI over publication of the group's results).

[32] *See* Webopedia, MP3, *at* http://webopedia.internet.com/TERM/M/MP3.html (last visited Dec. 17, 2003).

hostile platform while allowing the platform to 'play' the content, is inherent very difficult, both in theory and in practice. To overhaul their system, SDMI may well have to overhaul their business model."[33]

C. Trends in Digital Rights Management

Despite the readily apparent problems with copyright controls in the digital wild, the pursuit of and conflicts over DRM will only continue to escalate.

1. Business Trends

Digital technology simultaneously implicates the content industry's worst nightmares and its greatest hopes. In the pre-digital era, the unauthorized distribution of copyrighted works was cumbersome. Only professional counterfeiters achieved any continuous and widespread distribution. Computers and the Internet changed everything. Digital technology brought perfect copying functionality and easy worldwide distribution to even the most casual computer user. One only needs look as far as Napster and Peer-to-Peer file sharing to see that the public indeed wants to copy, share and distribute digital works.

The content industry sees DRM as the only possible hope in combating the continued, widespread copying of copyrighted digital works. George Colony of Forrester Research observes that "[w]e're entering a period of three to seven years where entertainment companies keep trying to control and consumers keep trying to escape it. ...

[33] Felten, *SDMI challenge FAQ*, *supra* note 30.

There's a lot of money at stake here and Hollywood doesn't want to lose it."[34] Jack Valenti, the prolific president of the Motion Picture Association of America, contends stronger digital protection is necessary for content providers: "We need to put in speed bumps to keep people honest[.] ... If we don't, our future is bleak."[35]

Not just a defensive measure, DRM also gives the content industry the possibility of reaping far more money and exercising far *greater* control over copyrighted works than was ever feasible in the pre-digital era.[36] Once a paper book is sold, the content industry is powerless to stop a consumer from reading the new book a particular number of times, owning the book for extended periods of times, and/or eventually selling the used book to someone else. DRM allows content owners to release the same book in digital file format, while retaining absolute control over the number of times the same consumer can view the file, keep the file on their computer, or transfer the digital file. Larry Kenswil, president of the eLabs division of Universal Music Group notes that under this new paradigm, "[y]ou're not buying [content], you're buying a key[.] ... That's what digital rights management does: it enables business models."[37]

Thus, creating more effective DRM is the veritable "holy grail" of technology for the content industry. DRM offers to plug the copyright holes of the digital age and give copyright owners unprecedented power over the public's use of digital content.

---

[34] Amy Harmon, *Studios Using Digital Armor to Fight Piracy*, N.Y. TIMES (Jan. 5, 2003), *available at* http://www.nytimes.com/2003/01/05/business/05CONT.html (last visited Mar. 30, 2003) [hereinafter Harmon, *Digital Armor*].
[35] *Id*.
[36] For a further discussion of the economic and social impacts of digital rights management, *see* Julie Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (Nov., 1998).
[37] Harmon, *Digital Armor, supra* note 34.

2. Technological Trends

Despite repeated failures, DRM technologies continue to proliferate, most notably in the area of digital music. Ed Felten and other researchers quickly dashed the hopes of SDMI as a DRM solution for music. John Borland, a technology writer, describes the same result for almost all CD copy protection schemes:

> [P]revious versions of the antipiracy technologies from SunnComm, Macrovision and others have proven flawed. CDs protected with the technology have been unable to play in some CD players or computers, potentially even damaging some machines. Hackers have been able to break through much of the protection technologies using techniques as simple as drawing on the CD with a felt-tipped pen.[38]

Nonetheless, imperfect DRM solutions are viewed as "deterrent[s]" until better technologies become available.[39] SunnComm and other DRM producers press on with new DRM technologies, hoping that maybe one time, it won't break.

While most CD DRM solutions have been confined to test markets, this is soon to change as well. A recent research note from J.P. Morgan analyst Sterling Auty expects "volume shipments of protected CDs to ship commercially in the U.S. as early as the May-June time frame using the SunnComm solution," and concludes that "[t]his will be the first major step in the growth of the CD audio protection market."[40] Likely responding to Auty's note, Macrovision claims that *already* over 100 million CD's in distribution worldwide are protected by its technologies.[41] Additionally, DRM

---

[38] John Borland, *Copyproof CDs Moving to Market?*, CNET News.com, *at* http://news.com.com/2100-1027-994565.html?tag=fd_top (last modified Mar. 28, 2003) [hereinafter Borland, *Copyproof CDs Moving to Market?*].
[39] Harmon, *Digital Armor*, *supra* note 34.
[40] *Id*.
[41] John Borland, *100 Million Copyproof CDs Sold?*, CNET News.com ("Silicon Valley company Macrovision said Wednesday that its anticopying technology had now been applied to more than 100 million CDs worldwide, the bulk of them released in Europe and Japan. Over the last six months, the company has seen shipments of 10 million discs a month distributed across those markets, it said."), *at* http://news.com.com/2100-1027-995200.html?tag=fd_top (last modified Apr. 2, 2003).

deployment continues in a multitude of other digital fronts, like DVD's[42], e-mail and word processing document files[43] and high-definition TV's ("HDTV's").[44]

The burning desire of the content industry for DRM is met by continued development from the technology industry. Technology companies with the most effective DRM stand to gain advantage in the digital content arena. Professor Ross Anderson summarizes the technology-entertainment industry relationship by way of an example of Intel:

> [Intel] makes most of its money from the PC microprocessor; they have most of the market; so to grow the company they need to grow the overall market for PCs; that means making sure the PC is the hub of the future home network; and if entertainment's the killer app, and DRM is the key technology for entertainment, then the PC must do DRM.[45]

However, not all of the technology industry tows the content industry line. Many technology companies make products that are attractive for their use of unprotected digital formats, and see DRM as antithetical to their interests. Also, some companies attempt for the best of both worlds. Although recently developing its own moderate DRM system for music files,[46] Daniel Steinberg notes that Apple "has been in the

---

[42] *See* Harmon, *Digital Armor*, *supra* note 34.

[43] Mary Jo Foley, *'Information Rights Management' To Debut in Office 2003*, Microsoft Watch (Feb. 21, 2003) (noting that Microsoft is testing "Information Rights Management" ("IRM") technology for Office 2003. According to a Microsoft testing code document, "IRM is a persistent file-level technology from Microsoft that allows the user to specify permission for who can access and use documents or e-mail messages, and helps prevent sensitive information from being printed, forwarded, or copied by unauthorized individuals[.] ... Once permission for a document or message has been restricted with this technology, the access and usage restrictions are enforced no matter where the information is."), *at* http://www.microsoft-watch.com/article2/0,4248,899456,00.asp.

[44] *See* Harmon, *Digital Armor*, *supra* note 34.

[45] Posting of Ross Anderson, Ross.Anderson@cl.cam.ac.uk, to cypherpunks@lne.com (June 24, 2002), *available at* http://cryptome.org/tcpa-rja2.htm.

[46] In late April, 2003, Apple Computer opened its "iTunes Music Store" (*at* http://www.apple.com/music/) offering a large collection of digital music files for download at 99 cents each. John Borland, *Apple Unveils Music Store*, CNET News.com (April 28, 2003), *at* http://news.com.com/2100-1027-998590.html?tag=fd_lede2_hed [hereinafter Borland, *Apple Unveils Music Store*]. The files are protected with moderate-level DRM protection, allowing users to burn their own CD's and transfer files a limited number of times. *Id*. The service has been quite popular since opening.

forefront of creative freedom and continues to enable creative expression with the suite of iApps," which enable editing and playback of a variety of digital content.[47]

Thus, despite its failures, DRM is the near-term and long-term goals of the content industry. And much of the technology industry has vested interests in creating DRM to meet these goals. Hilary Rosen, the former chief executive of the Recording Industry Association of America ("RIAA"), has the optimistic view that "[w]hile the technology is apparently not quite ready, there is promise for some protective technologies,"[48]

3. Legislative Trends

Weary of the technological limits of DRM solutions and the reluctance of some technology producers to embrace a complementary vision, the content industry has additionally pursued DRM through more malleable arena of politics. The content industry's failsafe plan is to politically reign in the public and dissenting technology companies that presently benefit from refusing DRM in popular products. J.D. Lasica, senior editor of the Online Journalism Review, observes that for content-embracing companies, "any opposition to content control is frowned upon in the halls of Congress. The film industry has the attention of the Congress and has thrown 60 million dollars at it."[49]

---

[47] Daniel H. Steinberg, *The Near Future of Digital Rights Management*, O'Reilly MacDevCenter.com (Oct. 3, 2002), *at* http://www.macdevcenter.com/pub/a/mac/2002/10/03/drm.html [hereinafter Steinberg, *Near Future*].
[48] Borland, *Copyproof CDs Moving to Market?*, *supra* note 38.
[49] Steinberg, *Near Future*, *supra* note 47 (discussing Apple).

a. Digital Rights Management Legislation

The content industry's cries are falling on receptive ears. In September of 2001, Senator Ernest "Fritz" Hollings (D-SC) scheduled a Congressional introduction for his bill, the Security Systems Standards and Certification Act ("SSSCA").[50] The SSSCA draft mandated DRM technology by creating civil offenses for the sale or creation of any computer that "does not include and utilize certified security technologies."[51] The SSSCA also enumerated new federal felonies for trafficking in copyrighted content with disabled "security measures."[52] On March 21, 2002, Senator Hollings introduced a modified version of the bill under a new title, the Consumer Broadband and Digital Television Promotion Act ("CBDTPA").[53] The CBDTPA mandates that every new electronic device short of a digital "clock"[54] have built-in DRM technology:

> [The CBDTPA] would have movie studios, record labels and others attach digital tags to a movie, song or album that would encode rules about how it could be played, viewed or copied on devices such as computers or digital TVs.
>
> Manufacturers and content owners would have a year to agree on technology to enforce these rules; after that, the Federal Communications Commission could impose a standard. It would then be illegal to manufacture devices that didn't implement it.[55]

In addition to Hollings' far-reaching gambit, many politicians have offered related legislation. Proposed legislation and rules range from mandating copy protection codes

---

[50] Declan McCullagh, *New Copyright Bill Heading to DC*, Wired News (Sept. 07, 2001), *available at* http://www.wired.com/news/politics/0,1283,46655,00.html.
[51] *Id*. (quoting the SSSCA).
[52] *Id*. (quoting the SSSCA).
[53] *See* Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2002); *see also* Mike Musgrove, *Hollings Proposes Copyright Defense*, Washington Post (Mar. 22, 2002), *available at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A92-2002Mar21&notFound=true [hereinafter Musgrove, *Hollings Proposes Copyright Defense*].
[54] Declan McCullagh, *Anti-Copy Bill Slams Coders*, Wired News (Mar. 22, 2002) (quoting Tom Bell, an intellectual property professor at Chapman University School of Law), *available at* http://www.wired.com/news/politics/0,1283,51274,00.html.
[55] Musgrove, *Hollings Proposes Copyright Defense*, *supra* note 53.

in digital television signals,[56] to permitting the content industry to pursue "government-sanctioned vigilantism" against online file sharing systems.[57] In July of 2002, Representative Howard Berman (D-CA) introduced an anti-piracy bill, H.R. 5211,[58] to combat Peer-to-Peer file sharing.[59] H.R. 5211 would allow *content owners* to attack and hack file traders believed to be trafficking in unauthorized copyrighted works. The bill would offer individuals "almost no recourse" if they were wrongly attacked by copyright owners.[60]

b. Anti-Digital Rights Management Legislation

Washington, however, is rarely on one side of an issue. Several legislators have proposed bills limiting the ability of content owners to implement DRM as well as prohibiting DRM-friendly legislation. On March 4, 2003, Representative Zoe Lofgren (D-CA) introduced H.R. 1066, the Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003.[61] The BALANCE act would include analog and digital transmissions of copyrighted content within the public's fair

---

[56] *See* EPIC, *Digital Rights Management and Privacy*, *supra* note 6 (noting that "[i]n August 2002, the FCC issued a notice of proposed rulemaking (NPRM) to consider whether digital television signals should incorporate a digital broadcast flag. Such a flag would mark digital content as "protected" and direct devices to limit individuals' use of the content.").

[57] Electronic Frontier Foundation, *The Berman P2P Bill: Vigilantism Unbound*, *at* http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html (discussing Representative Howard Berman's proposed bill, H.R. 5211) (last visited Dec. 18, 2003).

[58] H.R. 5211, 107th Cong. (2002).

[59] *See* EPIC, *Digital Rights Management and Privacy*, *supra* note 6.

[60] *Id*. (noting that "[a] wronged individual would first have to complain to the Department of Justice before bringing suit, and in order to prevail in court, the individual would have to show over $250 in monetary damages and that the copyright agent knowingly and intentionally blocked a legal file transfer.").

[61] Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003, H.R. 1066, 108th Cong. (2003). The BALANCE act was a reintroduction of Lofgren's earlier bill, the Digital Choice and Freedom Act of 2002, H.R. 5522, 107th Cong. (2002).

use protections,[62] allow end users to make digital backups,[63] and create a digital "first sale" doctrine.[64] Most importantly, the bill would allow the public to circumvent any copyright protection technology (like DRM) for purposes that are traditionally exempted under copyright law.[65] On March 24, 2003, Senator Ron Wyden (D-OR) introduced S. 692, the Digital Consumer Right to Know Act ("DCRKA"),[66] which would grant the Federal Trade Commission ("FTC") the power to regulate labeling of CD's with any form of content protection or DRM technology limiting public use.[67]

Representative Rick Boucher's (D-VA) earlier January 1, 2003 bill, H.R.107, Digital Media Consumers' Rights Act of 2003 ("DMCRA"),[68] encompasses elements of both the Wyden and Lofgren bills. The DMCRA requires "prominent and plainly legible" notice to consumers on copy-protected CD's, although Boucher's provision is not as wide-ranging as Wyden's DCRKA.[69] Similar to Lofgren's BALANCE Act, the DMCRA would create exceptions to the DMCA, allowing users to circumvent technology protection (like DRM) for noninfringing uses and for scientific research.[70] The DMCRA would further allow the manufacture and distribution of tools "capable of enabling significant noninfringing use of a copyrighted work."[71]

---

[62] *See id*. § 3 ("(a) FAIR USE- The first sentence of section 107 of title 17, United States Code, is amended by inserting after 'or by any other means specified in that section,' the following: 'including by analog or digital transmissions,'.").
[63] *See id.* § 3.
[64] *See id*. § 4.
[65] Contingent on the content owner not providing the means to allow currently legal noninfringing or fair uses of digital material. *See id*. § 5.
[66] Digital Consumer Right to Know Act, S. 692, 108th Cong. (2003).
[67] *See* Declan McCullagh, *Senator Calls For Copy-Protection Tags*, CNET News.com, *at* http://news.com.com/2100-1028-994176.html?tag=fd_top (last modified Mar. 26, 2003) [hereinafter McCullagh, *Senator Calls For Copy-Protection Tags*].
[68] Digital Media Consumers' Rights Act of 2003, H.R.107, 108th Cong. (2003).
[69] McCullagh, *Senator Calls For Copy-Protection Tags*, *supra* note 67; *see also* H.R. 107 § 3.
[70] *See* H.R. 107 § 5.
[71] *Id*.

c. Standoffs and Uneasy Truces

The technology industry is understandably worried about any legislative DRM mandates. Technology coalitions have been active in opposing the possible reintroduction of Sen. Holling's CBDTPA, which threatens the most far-reaching mandates.[72] Jack Valenti and the motion picture industry continue to support the bill, standing at odds with the technology community.[73]

The music industry, however, has been able to find a shaky middle ground with the technology industry. On January 14, 2003, the music industry and many technology groups agreed on a "rhetorical peace accord."[74] The music industry promised to forego pursuing DRM legislative mandates in exchange for the technology industry's restraint in seeking anti-DRM legislation.[75] Both groups agreed to pursue mutual technology and public solutions to digital content piracy, rather than resort to appeals to Washington.[76] For the time being, it appears that DRM legislation is being held at bay by the pushes and pulls from various interested coalitions.

II. Trusted Computing

The present technological failures of DRM are forcing the technology industry to consider new approaches. Most DRM security is implemented to secure software, but not hardware. The underlying hardware and operating system allow an end user to access

---

[72] *See* Declan McCullagh, *Tech Firms Fight Copy-Protection Laws*, CNET News.com, *at* http://news.com.com/2100-1023-981882.html?tag=fd_lede2_hed (last modified Jan. 23, 2003).
[73] *See id.*
[74] Declan McCullagh, *Antipiracy Detente Announced*, CNET News.com, *at* http://news.com.com/2100-1023-980633.html?tag=lh (last modified Jan. 14, 2003).
[75] *See id.*
[76] *See id.* ("Instead of fighting before Congress over what new laws are necessary, the groups say they'll work together to educate the public, sue pirates, and develop "unilateral technical protection measures that limit unauthorized access, copying or redistribution" of copyrighted materials.").

every bit of information in a digital file, even when protected by software DRM. With this low-level access, end users can attack the digital file itself, intercept digital information as a program executes (through an emulator or debugger), or access the end result (through screen or audio capture programs).

In December 1996, Bill Arbaugh, Dave Farber and Jonathan Smith published a paper entitled "A Secure and Reliable Bootstrap Architecture," describing the technical means to accomplish a secure hardware environment.[77] The idea, dubbed "trusted computing"[78] or "trustworthy computing," proposes adding several hardware components to computers to create greater security for encryption, storage and software.

A. Trusted Computing Platform Alliance

In 1999, a collection of hardware and software companies formed the Trusted Computing Platform Alliance ("TCPA") with the goal of transforming trusted computing research into a workable architecture for the PC.[79] The TCPA was created with the express goal of providing a single, common platform for trusted computing.[80]

---

[77] *See* Bill Arbaugh et al., *A Secure and Reliable Bootstrap Architecture* (Dec. 2, 1996), *available at* http://www.cis.upenn.edu/~waa/96-35/aegis.html (last visited Mar. 12, 2003). This research eventually led to a patent entitled "Secure and Reliable Bootstrap Architecture," U.S. Patent No. 6,185,678 (issued Feb. 6, 2001).

[78] The name "trusted" computing does not necessarily mean that a TC device is to be trusted by the end user. Rather it means a computer that could break the security in a given security relationship (like DRM). Ross Anderson describes the origins of the phrase as:

> ...almost an in-joke. In the US Department of Defense, a 'trusted system or component' is defined as 'one which can break the security policy'. This might seem counter-intuitive at first, but just stop to think about it. The mail guard or firewall that stands between a Secret and a Top Secret system can - if it fails - break the security policy that mail should only ever flow from Secret to Top Secret, but never in the other direction. It is therefore trusted to enforce the information flow policy.

Anderson, *TCPA / Palladium FAQ*, *supra* note 11.

[79] *See* Trusted Computing Platform Alliance, *Compaq, HP, IBM, Intel, and Microsoft Announce Open Alliance to Build Trust and Security into PCs for e-Business* (Oct. 11, 1999) ("The alliance's mission is the development of a new hardware and software specification that will enable technology companies to offer a more trusted and secure personal computer platform based on common standards."), *available at*

Despite some early contentions, TCPA does not actually control the execution of DRM programs.[81] TCPA simply protects the integrity of digital files and cryptographic keys, and guarantees that the hardware and low level operating state are in a known, "trusted" state.[82] Nonetheless, the TCPA trusted framework could enable developers to write very secure DRM programs.[83] A TCPA system could verify that DRM programs remain unaltered.[84] DRM developers could also utilize TCPA to seal and encrypt content files, ensuring access only by authorized means.[85]

TCPA provides a framework in which a computer starts up securely, verifies its individual components, and can verify this trusted state to third parties.[86] On boot up, a device attached to a PC's motherboard known as a Trusted Platform Module ("TPM") examines the PC's configuration.[87] This chip checks that all of the hardware is TCPA-

---

http://www.trustedcomputing.org/docs/tcpa_press_rel.7.pdf (last visited Apr. 2, 2003); *see also* Anderson, *TCPA / Palladium FAQ*, *supra* note 11; Trusted Computing Platform Alliance, *TCPA Frequently Asked Questions, Rev 5.0* (July 3, 2002) ("The TCPA is an industry working group, initially formed by Compaq, HP, IBM, Intel and Microsoft in October 1999 that is focusing on improving trust and security on computing platforms. Since that time, the TCPA has grown to over 150 participating companies."), *available at* http://www.trustedcomputing.org/docs/Website_TCPA%20FAQ_0703021.pdf [hereinafter TCPA, *TCPA FAQ*].

[80] TCPA, *TCPA FAQ*, *supra* note 79, ("What are the goals of the TCPA? Through the collaboration of hardware, software, communications and technology, vendors drive and implement TCPA specifications for an enhanced HW and Operating System based trusted computing platform that implements trust into client, server, networking, and communications platforms.").

[81] *See* Safford, *Clarifying Misinformation on TCPA*, *supra* note 5.

[82] *See id*.

[83] Anderson, *TCPA / Palladium FAQ*, *supra* note 11.

[84] *See* Safford, *Clarifying Misinformation on TCPA*, *supra* note 5, ("The 'trusted' boot functions provide the ability to store in Platform Configuration Registers (PCR), hashes of configuration information throughout the boot sequence. Once booted, data (such as symmetric keys for encrypted files) can be 'sealed' under a PCR.").

[85] *See id*.

[86] *See* Anderson, *TCPA / Palladium FAQ*, *supra* note 11; *see also* Trusted Computing Platform Alliance, *TCPA Specification/TPM Q&A*, *available at* http://www.trustedcomputing.org/docs/TPM_QA_071802.pdf (last modified July 18, 2002) [hereinafter TCPA, *TPM Q&A*].

[87] William Arbaugh, *The TCPA; What's wrong; What's right and what to do about*, *available at* http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.html (July 20, 2002) ("The Trusted Platform Module (TPM) is the core of the TCPA specification. ... The TPM is really nothing more than a cryptographic co-processor tightly coupled to the CPU that requires software support from the BIOS, and host operating system.").

compliant, and if so, the chip allows the computer to run in a "trusted" mode.[88] A TCPA system then checks out the entire computer, providing a report called an "attestation," which verifies the "current configuration of the platform."[89] The "[k]nowledge and confirmation of the current software running on a system" provided by attestation may be relayed to remote third parties.[90] DRM producers can use this attestation to guarantee that an end user's computer is a secure DRM environment.[91] The TPM module also creates a unique "identity" for the TCPA system.[92] This identity is sent to "Certification Authority" (CA's), also known as a "Trusted Third Party" (TPP), which generates a "certificate" for various uses by the end user.[93] Thus, the TCPA scheme enables third parties to identify and attest to the DRM security of end user's computers.

B. Trusted Computing Group

In April of 2003, several key members of the TCPA pulled out of the organization in order to form a new entity, the Trusted Computing Group ("TCG").[94] The TCPA's organizational goal was to develop a common technical specification for trusted computing systems. By contrast, TCG is focused on becoming "a more formal group

---

[88] Anderson, *TCPA / Palladium FAQ*, *supra* note 11.
[89] TCPA, *TPM Q&A*, *supra* note 86.
[90] *Id*.
[91] *See* Brian LaMacchia, *Key Challenges in DRM: An Industry Perspective*, ACM DRM Workshop, *available at* http://crypto.stanford.edu/DRM2002/abstract-bal.doc (last visited Dec. 22, 2002) [hereinafter LaMacchia, *Key Challenges in DRM*].
[92] *See* Wintermute, *TCPA and Palladium Technical Analysis*, at § 2.6.5, *at* - http://www.kuro5hin.org/story/2002/10/27/16622/530 (last visited Dec. 22, 2003) [hereinafter Wintermute, *TCPA and Palladium Technical Analysis*].
[93] *Id*. This system creates the potential for "serious privacy breach[es]" as a CA will necessarily be able to learn information about an end user in creating a certificate. *See id* (noting that despite the TCPA's claims, the TCPA-created identity could reveal personally identifying information about end users).
[94] Advanced Micro Devices, Hewlett-Packard, IBM, Intel and Microsoft pulled out of the TCPA on April 8, 2003. Robert Lemos, *Tech Giants Put Chips On Security Alliance*, CNET News.com, *at* http://news.com.com/2100-1009-996032.html?tag=fd_lede2_hed (last modified Apr. 8, 2003).

with licensing policy, a marketing budget, and a mission to push the trusted computing technology into a variety of devices."[95]

Upon its creation, TCG adopted the TCPA's present technical specifications as its own.[96] All further specification development will be pursued by the TCG.[97] Consequently, the TCPA organization acknowledges that "TCPA has recognized TCG as the industry standard organization that will work on future trusted computing specifications."[98]

C. Creating Trusted Systems

1. Trusted Computing Group Operating Systems

The TCG architecture controls internal aspects of a computer that an average computer user would never see - functions like boot up, memory access and storage, and cryptographic functions. TCG offers secure computing functions to the operating system or software programs to use as they see fit. A TCG subsystem is agnostic as to what operating system runs on top of its TCG components.[99] The first specification, TCPA version 1.1b (now TCG version 1.1b), only details the subsystem support for a trusted

---

[95] *Id*.
[96] Trusted Computing Group, *Trusted Computing Group: Frequently Asked Questions*, *at* http://www.trustedcomputinggroup.org/about/faq (last visited Dec. 22, 2003) ("TCG has adopted the existing TCPA specifications, including the Main (TPM 1.1) specification, and PC Specific Implementation specification. A TSS (TCG Software Stack) specification was announced on September 15, 2003. The TPM 1.2 specification was announced on November 5, 2003. Work Groups have been formed for server, PDA, and digital phone implementation specifications. A timeline for the completion of these has not yet been established.") [hereinafter TCG, *TCG: Frequently Asked Questions*].
[97] *Id*.
[98] *Id*.
[99] TCPA, *TPM Q&A*, *supra* note 86, ("The TCPA specification is designed to be platform and OS agnostic. The TCPA specification is not limited to a specific platform, OS or CPU.").

computer.[100] The next version of the TCG specification, 1.2, will include guidelines for trusted operating systems.[101] At that point, fully integrated TCG-enabled computers will become a reality. Technology companies are already forging ahead with the 1.1b specification, as well as preparing for the 1.2 specification. To date, IBM has released "driver" software to utilize TCPA components for the open source operating system, GNU/Linux ("Linux")[102], and several TCPA vendors are working on Linux TCPA Application Program Interfaces[103] ("API's").[104]

2. Microsoft's Next Generation Secure Computing Base

Despite belonging to both TCPA and TCG, Microsoft has its own vision for trusted systems. Microsoft is currently developing its own trusted computing system, the Next-Generation Secure Computing Base ("NGSCB") (formerly known as "Palladium").[105] NGSCB is not an actual implementation of a TCPA or TCG specification - it's more.[106] NGSCB attempts create both a TCG-like hardware

---

[100] Jan Ozer, *Trusted Computing*, Baseline (Feb. 1, 2003), *at* http://www.baselinemag.com/article2/0,3959,887902,00.asp [hereinafter Ozer, *Trusted Computing*].
[101] *Id*.
[102] *See* Safford, *Clarifying Misinformation on TCPA*, *supra* note 5, ("...TCPA already has a freely downloadable detailed specification, and a tested port of all driver and library level software to Linux.").
[103] The Webopedia defines "API" as:

> Abbreviation of *application program interface*, a set of routines, protocols, and tools for building software applications. A good API makes it easier to develop a program by providing all the building blocks. A programmer puts the blocks together.
> Most operating environments, such as MS-Windows, provide an API so that programmers can write applications consistent with the operating environment.

Webopedia, API, at http://www.webopedia.com/TERM/A/API.html (last visited Dec. 22, 2003).
[104] *See* Paul Krill, *Linux boost expected for Trusted Computing scheme*, InfoWorld (January 29, 2003), *available at* http://www.infoworld.com/article/03/01/29/hntcpa_1.html.
[105] Microsoft change the name of their trusted computing system from "Palladium" to "next-generation secure computing base," in January of 2003. Robert Lemos, *What's in a name? Not Palladium*, CNET News.com (Jan. 24, 2003), *at* http://news.com.com/2100-1001-982127.html?tag=fd_top. Many observers continue to use the term "Palladium" in lieu of the unwieldy acronym, NGSCB.
[106] Microsoft, *Microsoft Next-Generation Secure Computing Base - Technical FAQ* (Feb., 2003) ("No, NGSCB is not an implementation of the existing specifications developed by TCPA or TCG. The upcoming version of the trusted platform module (TPM 1.2) is expected to work as the security support

subsystem, as well as a trusted operating environment. NGSCB creates a "secure, parallel" operating system[107], known as the "Nexus," which runs alongside the Windows operating system.[108] When an application requires "trusted" features, NGSCB verifies the state of the computer and performs trusted computing functions.[109] Technically, NGSCB implements four main security features:

> Strong process isolation. Users can wall off and hide pages of main memory so that each nexus-aware application can be assured that it is not modified or observed by any other application or even the operating system.
>
> Sealed storage. Information can be stored in such a way that only the application from which data is saved (or a trusted designated application or entity) can open it. With sealed storage, a nexus-aware application or module can mandate that the information be accessible only to itself or to a set of other trusted components that can be identified in a cryptographically secure manner.
>
> Secure path to and from the user. Secure channels allow data to move safely from the keyboard/mouse to nexus-aware applications, and for data to move from nexus-aware applications to a region of the screen.
>
> Attestation. Users have the ability to authenticate software or a combination of software and hardware. With attestation, a piece of code can digitally sign or otherwise attest to a piece of data and thus assure the recipient that the data was constructed by an unforgeable, cryptographically identified trusted software stack.[110]

The bulk of the NGSCB hardware design is "remarkably similar" to the original TCPA specification, utilizing a separate chip to control the trusted system, new encryption

---

component in the NGSCB architecture."), *at* http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/NGSCB.asp (last visited Jan. 6, 2004) [hereinafter Microsoft, *Microsoft NGSCB - Technical FAQ*].

[107] John Lettice, *Inside Microsoft's Secure OS Project Palladium*, ExtremeTech (Nov. 12, 2002), *at* http://www.extremetech.com/article2/0,3973,837726,00.asp (last visited Dec. 26, 2003) [hereinafter Lettice, *Inside Microsoft's Secure OS Project Palladium*].

[108] John Lettice, *Of TCPA, Palladium and Werner von Braun*, The Register (Aug. 11, 2002), *at* http://www.theregister.co.uk/content/4/28016.html (last visited Dec. 26, 2003) [hereinafter Lettice, *Of TCPA, Palladium and Werner von Braun*].

[109] *See* Microsoft, *Microsoft NGSCB - Technical FAQ*, *supra* note 106.

[110] *Id*.

functions, and sealed memory.[111] NGSCB hardware module is called a "Security Support Component" ("SSC"), which comprises the same basic functionality as TCPA's TPM.[112] Beyond the current TCG specification, NGSCB introduces the idea of "Notarized Computing Agents" ("NCA's").[113] The NGSCB Nexus runs all of the NCA's for a given computer.[114] NCA's are essentially subsets of larger software applications that are responsible for attesting that a computer is "safe" for a program and accessing secure memory storage.[115]

The NGSCB system is developing rapidly. Microsoft demonstrated the preliminary system and technical details in May, 2003 at the Windows Hardware Engineering Conference.[116] It is speculated that NGSCB may be released as a part of the Windows operating system in 2005, with other Windows DRM operating system components being released this year.[117]

3. A Complete Package: Approaching a Secure Trusted Computing Environment

TCG provides the basic hardware framework for a trusted computer. However, trusted computing advocates "admit that without operating system support, they can only ensure a trusted state through boot-up."[118] For DRM to utilize the full security of trusted

---

[111] *See* Robert Lemos, *MS Palladium: A Must or a Menace?*, ZDNet (Nov. 7, 2002), *at* http://zdnet.com.com/2100-1105-964876.html [hereinafter Lemos, *A Must or a Menace?*].
[112] *See id.*
[113] Lettice, *Inside Microsoft's Secure OS Project Palladium*, *supra* note 107.
[114] Lettice, *Of TCPA, Palladium and Werner von Braun*, *supra* note 108.
[115] *Id.*
[116] *WinHEC 2003 Trusted Platform Technologies Sessions*, Microsoft Corporation, *at* https://www.microsoft.com/whdc/winhec/trusted03.mspx (last updated June 13, 2003); *see also* Mary Jo Foley, *Microsoft To Demo 'Palladium' At WinHEC*, Microsoft Watch (Mar. 26, 2003), *at* http://www.microsoft-watch.com/article2/0,4248,976208,00.asp (last visited Dec. 26, 2003) [hereinafter Foley, *Microsoft To Demo 'Palladium' At WinHEC*].
[117] *See* Foley, *Microsoft To Demo 'Palladium' At WinHEC*, *supra* note 116.
[118] Ozer, *Trusted Computing*, *supra* note 100.

computing, a secure framework must be available the entire time a computer is operating. Thus, regardless of whether NGSCB catches public favor, or if an operating system born out of TCG specification 1.2 becomes prevalent, trusted operating systems will become the final piece in implementing a secure environment for DRM.

III. Technological Limitations at the Intersection of Trusted Computing and Digital Rights Management

A. Securing Digital Rights Management with Trusted Systems

NGSCB demonstrates that trusted systems are a forerunner to stronger DRM frameworks. Although Microsoft eschews that "NGSCB is not DRM," it admits that "DRM applications can be developed on systems that are built under the NGSCB architecture."[119] In December, 2001, Microsoft received patents for a "Digital Rights Management Operating System,"[120] and for "Loading and Identifying a Digital Rights Management Operating System."[121] It is unlikely that NGSCB presently will implement the DRM Operating System envisioned in Microsoft's patents, but like TCG, the NGSCB infrastructure makes DRM technologies more robust against cracking. Microsoft concludes that:

> The operating system and hardware changes introduced by NGSCB offer a way to isolate applications (to avoid snooping and modification by other software) and store secrets for them while ensuring that only software trusted by the person granting access to the content or service has access to the enabling secrets. A DRM system can take advantage of this

[119] Microsoft, *Microsoft NGSCB - Technical FAQ*, *supra* note 106.
[120] "Digital Rights Management Operating System," U.S. Patent No. 6,330,670 (issued Dec. 11, 2001).
[121] "Loading and Identifying a Digital Rights Management Operating System," U.S. Patent No. 6,327,652 (issued Dec. 4, 2001).

> environment to help ensure that content is obtained and used only in accordance with a mutually understood set of rules.[122]

Using a trusted computing environment, DRM developers can create programs that implement content restrictions on digital files.[123] It is no surprise then that DRM developers are watching closely the development of TCG and trusted systems. Brian LaMacchia of Microsoft contends that the most critical needs of DRM systems are "trustworthy computing devices, robust trust management engines and a general-purpose rights expression/authorization language."[124] Developers must then create systems (or "engines") which can determine which rights to grant users for digital files and which uses are restricted by the content owner.[125] LaMacchia poses that the technology community should agree on a common language which programs will understand, so that content owners can designate DRM rights and restrictions once for every DRM system and trusted platform, rather than specifying authorization for every different program that could use a single digital file.[126] Presently, the eXtensible rights Markup Language or ("XrML") is the forerunner with the Organization for the Advancement of Structured Information Standards ("OASIS"), the association that coordinates standards for XML languages.[127]

---

[122] Microsoft, *Microsoft NGSCB - Technical FAQ*, *supra* note 106.
[123] *See* LaMacchia, *Key Challenges in DRM*, *supra* note 91.
[124] *Id*.
[125] *See id.*
[126] *See id.*
[127] *See* Clint Boulton et al., *OASIS Sets Sights on XML for DRM*, Internetnews.com (Apr. 2, 2002) (Josh Duhl, an analyst notes that "'[t]he contribution of XrML to OASIS is an important step in establishing a standard rights language for DRM.'" The article concludes that "[m]ajor firms agree. ... the company with the most influence within the new rights management committee is ContentGuard, which uses an eXtensible rights Markup Language (XrML)"), *at* http://www.internetnews.com/dev-news/article.php/10_1002301.

Joe's simplified experience with a trusted computer running a DRM program is as follows: When Joe's TCG or NGSCB computer starts up, the trusted boot up device performs checks the hardware and software in Joe's computer. If Joe has changed nothing in his computer, then the trusted system will validate any "certificate" he has received from a CA (like Disney) and allow him to use his DRM software in the same manner as the last time he used his computer. If Joe *has* changed either the software or hardware, then the trusted system will detect this when it tries to access the certificate, and any certificates that relied on that particular component (hardware or software) will no longer work. If Joe replaced his TCG / NGSCB-compliant sound or video cards with ones that allowed him to record the sound or video output in digital form in an unrestricted manner, his trusted computer would attest to third parties that the sound or video cards had been changed. If Joe attempted to hack the code of his Disney-approved video viewing program, the changes to his viewing program would be detected by the trusted system, and Disney could invoke protections that prevented the program and digital files from any further use. Thus, if Joe's computer changes in any way that might threaten digital rights protection, Disney is empowered to stop Joe from viewing Snow White. Additionally, because the Snow White digital file was protected using trusted system encryption, Joe cannot use any *other* video program not explicitly authorized by Disney to view Snow White.

Now, if Joe wishes to view Snow White with his changed computer system, he must renegotiate with a CA (maybe Disney directly, or Microsoft, the company that produced the DRM program viewer) for a new certificate. If Joe's new system configuration checks out, the CA gives a new certificate and Joe may happily watch

Snow and her companions. If Joe's new system is not trusted by the CA (at Disney's or Microsoft's behest), then Joe cannot watch Snow White with his new system configuration. Joe's only option is to change all of the hardware / software back to its original state in which it was initially approved. Thus, Disney has complete control over Joe's viewing because Disney can verify that Joe's hardware configuration and for software, Joe *must* use a Disney-authorized video viewing program - one that respects Disney's DRM commands for Joe's file.

The trusted computing initiative provides several critical components missing from DRM systems. The TCG and NGSCB architectures provide a secure computing base that takes care of the ever-pressing encryption and verification needs of DRM. Trusted computing engines provide content owners with a funnel to force end users to access DRM files only through authorized DRM programs. And common rights expression languages enable content owners to have an easy and efficient means of communicating DRM rights and restrictions to software programs.

B. The Inherent Insecurity of Bits Revisited

Although trusted computing offers a giant leap forward for security for PC's, it will not be the final piece in the DRM-content puzzle. While this trusted computing enables far stronger DRM than currently available, the model is not likely to be secure against all attackers. In fact, it is likely that completely effective DRM is technologically impossible, both now and in the future.

1. Breaking Once and Breaking Everywhere

Darko Kirovski, a security researcher at Microsoft, observes that "[e]very single device has to be secure ... [i]f one device is not secure, then [DRM] doesn't work."[128] As discussed *supra*, in virtually every computer-based DRM system trotted out to the present, cracking one single digital file essentially renders the *entire* protection scheme insecure under Professor Felten's Napsterization threat model. If Joe finally gets fed up with Disney and successfully cracks his Snow White digital file, then he has individually broken the DRM system. If Joe can change the format of Snow White to something that plays on anyone's computer, then Disney's *entire* DRM protection has been compromised. A DRM system must therefore be BOBE-resistant (break-once, break-everywhere) to meet the Napsterization threat model. If a DRM system is unable to prevent BOBE-type attacks, then protected content will always be insecure. At this point, the best a DRM system can hope for is to look for a possible solution under the casual-copying model. However, the difficulty with using a near-perfect DRM model with existing technology is that popular digital content has the proclivity to spread rapidly worldwide.

2. Trusted Computing Cannot Completely Protect Digital Rights

Trusted computing is an incomplete answer to an issue that requires a complete solution. Content that has been encrypted and stored securely by a trusted computer can still be hacked. Microsoft NGSCB general manager John Manferdelli has acknowledged

[128] Robert Lemos, *Is Hardware Key To Piracy Crackdown?*, CNET News.com (Mar. 22, 2002), *at* http://news.com.com/2100-1023-867270.html (last visited Dec. 26, 2003).

that the NGSCB does not secure content against "sophisticated hardware attacks."[129] The TCG has similarly noted that "[i]t is not a goal of the TCG to enable or embed digital rights management (DRM) technology in computing platforms."[130] David Safford of IBM's Global Security Analysis Lab, concludes that :

> [T]he TCPA chip is not well suited to DRM tasks, and IBM's implementation of the chip was neither designed not [sic] evaluated for the necessary tamper resistance needed to provide effective copy protection (Personally, I do not believe it is possible do [sic] provide effective copy protection at all, but that's another paper).[131]

Additionally, both TCG and NGSCB, as presently specified, will continue to allow the use of unprotected content. TCPA/TCG Specification 1.1 does not even provide an operating system. Because the TCG functions can only be *called* by a program or operating system, TCG itself cannot restrict unauthorized or unprotected content from use on an end user's computer. Microsoft contends untrusted digital files (like MP3's) are safe because NGSCB does not interact in any way with untrusted programs.[132] Thus, TCG and Palladium will play hacked content, even if formerly protected by trusted computing. Consequently, trusted computing cannot guarantee effective DRM under a Napsterization threat model.

Moreover, technologies tend to bring unintended consequences and applications not previously conceived. In a strange twist of irony, a group of Harvard researchers have determined that trusted computing could be used to create a secure Peer-to-Peer file

---

[129] Lettice, *Of TCPA, Palladium and Werner von Braun*, *supra* note 108, (quoting John Manferdelli).
[130] TCG, *TCG: Frequently Asked Questions*, *supra* note 96.
[131] Safford, *The Need for TCPA*, *supra* note 2.
[132] *See* Microsoft, *Microsoft NGSCB - Technical FAQ*, *supra* note 106, ("Q: Will I still be able to play MP3s on my PC with NGSCB? A: You will. NGSCB will not interfere with the operation of any program that runs on current PCs. The nexus and nexus computing agents are designed never to impose themselves on processes that do not request their services; nexus-related features must be explicitly requested by a program. So the MP3 player a user has today should by design still work on a next-generation PC tomorrow").

sharing system.[133] This new secure system could be used by digital pirates to further circumvent copyright restrictions on digital works and protect their activities.[134]

3. The Possibility that *No* Technology Can Secure Digital Rights Management

The security experts opine that these past and predicted future DRM failures are a systematic indication. By the time that end users compromise trusted computers to a large degree, the content industry will likely move on to the next, more secure technology base for DRM systems. However, as long as the public can play unprotected content, only *one* break is necessary to have a worldwide DRM failure. And, securing against this last, single break is difficult - in fact, many experts say it is fundamentally *impossible* as a technical matter. Cryptography expert Bruce Schneier of Counterpane Internet Security contends that:

> Abstractly, [secure DRM] is an impossible task. All entertainment media on the Internet (like everything else on the Internet) is just bits: ones and zeros. Bits are inherently copyable, easily and repeatedly. If you have a digital file -- text, music, video, or whatever -- you can make as many copies of that file as you want, do whatever you want with the copies. This is a natural law of the digital world, and makes copying on the Internet different from copying Rolex watches or Louis Vuitton luggage.[135]

And therein lies the problem. Whatever Disney does to prevent Joe from hacking Snow White doesn't really matter if Joe has the *bits*, the actual digital content, on his computer. Eventually, Joe (or someone) will crack those bits, because they are out of Disney's

---

[133] *See* Stuart E. Schechter et al., *Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment*, *available at* http://www.eecs.harvard.edu/~stuart/papers/eis03.pdf (May 3, 2003) ("Can peer-to-peer networks be made immune from malicious client software written by the attacker? They can if the personal computer industry delivers on its promise of remote attestation. Though this technology was envisioned to thwart pirates, it is exactly what a peer-to-peer system needs to ensure that no client application can enter the network unless that application, and the hardware (not a virtual machine) and operating system it is running on, has been certified by an authority trusted by the existing clients.").
[134] *See id.*
[135] Schneier, *The Futility of Digital Copy Prevention*, *supra* note 1.

control. Even if encrypted. Even if in hardware. And when Joe eventually releases the unprotected, hacked version of Snow White on a file sharing network, the game is up. Snow White is unprotected and available for any member of the public to use without Disney's control. If present DRM cannot, as a technological matter, ever be secure then the content industry cannot rely on the Napsterization threat model to solve their digital content woes. Consequently, the content industry must look elsewhere to fill the technological gaps that cannot be solved or change their ambitions regarding copyrighted digital content.

C. Mixed Approaches for Enforcing Digital Rights

Although the pure technical question of DRM may be intractable, the content industry also relies on market, political and legal forces to address the shortcomings of DRM. Through a combination of DRM technology and these forces, the content industry may be able to address the difficulty of the Napsterization threat model, or possibly find a viable scenario for profiting under a casual-copying model.

The content industry can hope that sheer market force of DRM products can force out older non-DRM technologies over time or that trusted computing implementations will one day restrict all unprotected content. Presently TCG and NGSCB allow an end user to run in "untrusted" mode and access protected files. But, if new, DRM-protected content formats become ubiquitous, then the fact that a few stragglers can access unprotected content wouldn't matter as much. Bruce Perens, an open source software advocate, predicts that once DRM technologies cross a certain threshold of popularity, the public will all fall in line because without the new, DRM-friendly technology "you are an island .. [y]ou can't communicate with others. Everyone will be using this DRM,

and you can't view Web pages."[136] The actual threshold for such a displacement is still up in the air. The public's love of unprotected digital content and file sharing networks raises doubts about changing this model. But, the dominance of large technology producers, like Microsoft, which could arguably force a DRM system on consumers, may be able to reign in a large amount of the public. Either way, the content and technology industries are walking a delicate line - effective DRM products must restrict unauthorized use, but DRM with too many restrictions will likely never gain enough popularity to displace unprotected digital technologies.

From the legislative perspective, Sen. Holling's CBDTPA would secure DRM systems against even the Napsterization threat model, at least on paper. Mandating built-in copyright protection mechanisms still wouldn't prevent the cracking of individual digital files. But, if all computers contained strict digital copyright controls, a single cracked file couldn't be effectively played by the vast majority of the world. And, given the CBDTPA's severe civil and criminal sanctions, it is unlikely that average computer user would tinker with their hardware to access unprotected digital content. However, the expansive scope of the bill that would solve the content industry's DRM problems necessarily creates such a burden on the technology industry and public that any serious push for the bill would be met with enormous dissent.[137] Even without Holling's CBDTPA or any of the other current pro-DRM bills, the content industry has several

---

[136] Farhad Manjoo, *Can we trust Microsoft's Palladium?*, Salon.com (July 11, 2002), *at* http://www.salon.com/tech/feature/2002/07/11/palladium/?x (last visited Dec. 26, 2003).

[137] Jeff Grove, *New Legislative Attempt to Regulate Technology Poses Additional Threats to Access*, Association for Computing Machinery (2002) (noting that "heavy opposition from the IT industry combined with the ongoing concerns of computing and consumer groups dampens the prospects of congressional action on the CBDTPA this year."), *at* http://www.acm.org/membernet/stories/cbdtpa.html (last visited Dec. 26, 2003).

existing legal resources from which it could possibly bolster developing DRM technologies against attempts to circumvent digital content protections and controls.

IV. Copyright Law and Digital Circumvention

Copyright law strives to balance public access to works with creating incentives to produce by giving content owners a limited monopoly on copyrighted works.[138] Presently, copyright law is at the center of a fierce debate between content owners, technology producers and the public over emerging digital technologies. Professor Jessica Litman observes that the "pressures put by new technology on the current copyright statute have sparked disputes over whether the current copyright statute can adjust to the climate of rapid technological change."[139] Digital rights management technologies are inherently tied to copyright principles, as a technical means of enforcing legal rights of content owners.

A. Traditional Copyright Law

The United States guarantees several exclusive rights to copyright owners including the rights of reproduction, preparation of derivative works, distribution, performance and display.[140] The copyright owner subsequently has legal rights against parties who infringe on any of these rights, whether directly or indirectly.[141]

---

[138] Jessica Litman, DIGITAL COPYRIGHT 17 (Prometheus Books 2001) ("The system is premised on the assumption that we can give authors and their publishers rights to control some ways of exploiting their works, and reserve the rests of the value to the public at large.").
[139] *See id*. at 35.
[140] 17 U.S.C. § 106 (2003).
[141] *See id*. § 501(a) ("Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 122, or of the author as provided in section 106A(a), or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright or right of the author, as the case may be.").

However, copyright owners lack absolute control over their content. There are several exceptions to the basic exclusive rights of copyright law. The first sale doctrine allows a member of the public who has legally obtained a copyrighted work to resell the work without the copyright owner's authorization.[142] The fair use doctrine, which is called by some observers as "the single most important set of legal principles" in copyright law, allows a person to disregard copyrights for "fair use" situations, like study and criticism.[143] Fair use situations are often complicated due to the overwhelming disagreement on what constitutes a fair use.[144] The codification of the fair use doctrine, 17 U.S.C. § 107, purports to include such uses as "criticism, comment, news reporting, teaching ... , scholarship, or research" while leaving the ultimate fair use determination up to a number of factors.[145]

B. The Digital Millennium Copyright Act

In 1998, the U.S. Congress passed the Digital Millennium Copyright Act ("DMCA"), to bring copyright law up to date with modern digital technology.[146] The DMCA created conditional immunity for internet service providers,[147] added protections for "copyright management information,"[148] and addressed several other digital issues.

---

[142] *See id.* § 109(a) ("Notwithstanding the provisions of section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.").
[143] Stuart Biegel, BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 294 (Massachusetts Institute of Technology 2001) [hereinafter Biegel, BEYOND OUR CONTROL?]; *see also* 17 U.S.C. § 107 (2003).
[144] Biegel, BEYOND OUR CONTROL?, *supra* note 143, at 294 ("Yet it remains one of the most nebulous areas of this law, and court decisions in this area are filled with unusual and arguably inconsistent interpretations of what might actually constitute fair use.").
[145] 17 U.S.C. § 107.
[146] *See* Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).
[147] *See* 17 U.S.C. § 512.
[148] *See id.* § 1202.

Most importantly, the DMCA created an entirely new area of liability for the "circumvention of copyright protection systems".[149] Section 1201(a)(1)(A), the individual access prohibition, prevents anyone from circumventing a technology that "controls access" to a copyrighted work.[150] Section 1201(a)(2), the access circumvention tool prohibition, forbids the manufacture or distribution of any technology "primarily designed" to defeat the access controls to digital copyrighted content.[151] Section 1201(b)(1), the copy circumvention tool prohibition, similarly forbids distribution of any technology "primarily designed" to defeat "copyright" controls to a digital copyrighted work.[152] Essentially, DMCA anti-circumvention prevents *any* cracking of DRM technology that controls *access* to a work (individual access prohibition and access circumvention tool prohibition), and prohibits only the *distribution* of tools that crack DRM *copy* abilities. The only absent liability is that DMCA anti-circumvention permits *individual* cracks of DRM technology that controls copy abilities. Unfortunately, the line between what is an access protection and what is a copy protection is quite unclear at this time. The DMCA backs this broad new set of liabilities with traditional copyright remedies of damages, injunctive relief, special damages, and, in some cases, criminal penalties.

The DMCA contains some narrow anti-circumvention exceptions. Circumvention is permissible for reverse engineering where "program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve

[149] *Id*. § 1201.
[150] *Id*. § 1201(a)(1)(A).
[151] *Id*. § 1201(a)(2).
[152] *Id*. § 1201(b)(1).

interoperability" with other programs.[153] Circumvention is also allowed in certain, specific situations for encryption research[154] and security testing.[155] However, professor Pamela Samuelson notes that these exemptions "are very narrowly drawn and fail to recognize many legitimate reasons for circumventing technical measures[.]"[156]

C. The DeCSS Case

The DMCA's anti-circumvention provisions have only been tested in only a handful of cases. The most significant anti-circumvention case to date arose over the encryption in DVD's. DVD's, which typically contain digital movies, are encrypted with a DRM technology known as Content Scramble System ("CSS").[157] CSS ostensibly prevents DVD's from being unencrypted on unauthorized DVD players. In September, 1999, Jon Johansen cracked the CSS system and released a program, DeCSS, which enabled unfettered access and decryption of DVD's.[158] Johansen released DeCSS to the public, which quickly redistributed the program over the Internet. In November, 1999, Eric Corley posted the DeCSS program and links to other DeCSS copies on the website of the hacker magazine, *2600*.[159]

---

[153] *Id*. § 1201(f).
[154] *Id*. § 1201(g).
[155] *Id*. 1201(j).
[156] Pamela Samuelson, *Digital Rights Management {and, or, vs.} the Law*, 46 Comm. ACM 4, at 41-45 (April 2003), *available at* http://www.sims.berkeley.edu/~pam/papers/acm_v46_p41.pdf [hereinafter Samuelson, *Digital Rights Management and/or/vs. the Law*].
[157] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 308 (S.D.N.Y. 2000).
[158] *Id*. at 311; Johansen was tried and acquitted in Norway for the creation of the DeCSS program. His case has been appealed and is currently scheduled for retrial. *See* Reuters, *Teen Faces New Trial In Piracy Case* (April 1, 2003), *at* http://news.com.com/2102-1026_3-994919.html?tag=st_util_print (last visited Jan. 6, 2004).
[159] *See* Reimerdes, 111 F. Supp. 2d. at 311, 309.

The eight major motion picture studios promptly sued Corley and *2600* in New York district court in *Universal City Studios, Inc. v. Reimerdes* ("*Universal I*").[160] The motion picture studios claimed that the distribution ran afoul of the DMCA's anti-circumvention provisions for distribution of access and copy control circumvention device.[161] In addition to several constitutional claims, the defendants argued that DeCSS was exempted under the 17 U.S.C. § 1201 statutory exceptions and fair use. The district court was not persuaded. Initially, the defendants claimed that DeCSS was protected reverse engineering, necessary to play DVD's on the Linux operating system (which, at that time, did not have a DVD player). The court denied the exception, noting that the defendants had failed to prove that "the 'sole' purpose of DeCSS was to create a Linux DVD player[]" because "DeCSS concededly was developed on and runs under Windows--a far more widely used operating system."[162] The court similarly made short work of the defendants' encryption research and security testing exemption claims, holding the defendants' bad faith in posting the code forfeited both defenses.[163] Finally, the defendants claimed that DeCSS was necessary for the public to exercise traditional fair use because the CSS encryption scheme uniformly prohibited *all* unauthorized conduct. However, the court responded that:

> Access control measures such as CSS do involve some risk of preventing lawful as well as unlawful uses of copyrighted material. Congress, however, clearly faced up to and dealt with this question in enacting the DMCA.[164]

---

[160] *See id.*
[161] *See id.* at 316 (plaintiffs' 17 U.S.C. § 1201(a)(1) and 17 U.S.C. § 1201(a)(2) claims); *see also id.* at 316 n.133 (plaintiffs' 17 U.S.C. § 1201(b) claim).
[162] *Id.* at 319-20.
[163] *See id.* at 320-21.
[164] *Id.* at 322.

The court concluded that although fair use may provide some defense for traditional *infringement* claims, Congress had clearly intended to entirely foreclose the fair use doctrine for 17 U.S.C. § 1201(a) *anti-circumvention* claims.[165] Accordingly, the district court found that the defendants had violated the DMCA and awarded the motion picture studios an injunction against Corley or 2600 posting the DeCSS program or links to it.

The defendants appealed to the Second Circuit in *Universal City Studios, Inc. v. Corley* ("*Universal II*").[166] Examining only free speech issues and a narrow fair use question, the Second Circuit affirmed all of the district court's findings.[167] The Second Circuit upheld the constitutionality of the district court's fair use analysis, opining that the defendants had not made a credible fair use claim. The court concluded that "the Supreme Court has never held that fair use is constitutionally required" and moreover, that "[f]air 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."[168]

V. Building Blocks, Arms Races and Free-For-All's: Digital Copyright Law in a Trusted Computing Environment

Much has been written on drastic implications of DRM for copyright law and privacy issues.[169] Academics have theorized about what perfect DRM systems may

---

[165] *See id.* ("Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are "not . . . infringement[s] of copyright." Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.").

[166] Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[167] *Id.* at 459-60.

[168] *Id.* at 458, 459.

[169] This paper will not discuss the privacy implications of DRM or trusted computing. For an in-depth examination of the impact of DRM on privacy, *see* Julie Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 [hereinafter Cohen, *DRM and Privacy*]; *see also* EPIC, *Digital Rights Management and Privacy*,

entail and what they might imply for the public should they ever arrive. However, given the stunning failures of all previous wide-scale DRM attempts, the issue has been largely, well, academic. Until now. Trusted computing, although not complete, is real and coming soon. Within the next few years, trusted computing technology will make its way into the hardware of computers and electronic devices. Whether or not trusted computing was intended to promote DRM is simply a side issue for copyright law. Like other emerging technologies, trusted computing provides new capabilities that can be exploited by DRM producers and create new tensions within the legal system.

A. DMCA Anti-Circumvention Liability and Trusted Computers

Trusted computing systems, as seen through the development of TCG and NGSCB, disaggregate the security and protection tools from the actual DRM products. Unlike CSS, where the DRM system uses specific encryption functionality to protect a DVD, trusted computing security schemes are largely implementation-agnostic. TCG will use the same encryption techniques and attestation for a web browser to keep a credit card secure for online e-commerce as Disney utilizes to keep Joe from unauthorized access of Snow White. There is no design or purpose in the encryption, sealing and attestation functions of trusted computing.

1. Scenarios of Attack: Circumventing Digital Rights Management Protections on a Trusted Computer

It is also important to consider how an end user might actually circumvent the security of a DRM program based on a trusted system. At the most basic level, a hacker

---

supra note 6. For a technical description of the privacy problems in TCPA and Microsoft's Palladium technologies, *see* Wintermute, *TCPA and Palladium Technical Analysis*, *supra* note 92.

could attempt to circumvent the trusted computing hardware subsystem. As described above, it is possible for experts to access *individual* digital files.[170] However, an individual crack of a file on a trusted computer doesn't compromise the file on other computers, or other files on the original trusted computer.[171] An attack on the *whole* system (like DeCSS) does not presently appear possible for trusted systems.[172] And, a hack on the trusted subsystem would change some of the hardware or software values that would be used to attest the state of the computer to a third party.

Moving up a level, a hacker could attempt to write an interoperable program to use DRM-protected files without authorization or attack the DRM program. Jon Johansen's DeCSS successfully accessed the digital content of encrypted DVD digital files. However, with trusted computing, a DRM program and its files are protected by the *trusted computing system*, not the DRM program itself (like CSS).[173] Thus, if the trusted computing scheme is effectively utilized by DRM producers, this method of attack ultimately defaults a hacker back to the initial (and quite difficult) option of hacking the trusted hardware system.

---

[170] See earlier discussion where TCPA and Microsoft both admit vulnerabilities to hardware-specific attacks.

[171] The fact that *attacks* on trusted files cannot be replicated on a system level may appear to meet Prof. Felten's Napsterization threat model, but this is not the case. Once an individual trusted file is hacked, the hacker can then convert the file into an unprotected format (like MP3's for music). Thus, although the trusted computing may be resistant to system-wide attacks on individual files, they do not guarantee that one cracked file won't appear in a different form on the Internet.

[172] An analysis of the actual robustness of either TCPA or NGSCB against hacking the entire system is beyond the scope of this paper. Additionally, actual attacks would be speculative, as trusted specifications are still under development. That said, the systems appear quite robust. For a technical examination of the security components and implementations of TCPA and Palladium, *see* Wintermute, *TCPA and Palladium Technical Analysis*, *supra* note 92.

[173] Of course, DRM producers could always make errors in their use of the trusted computing security and this could be attacked. DMCA liability would fall along the lines of the DeCSS case. However, trusted computing makes this very unlikely. Security of DRM files is left to the trusted system *and* any attempts to hack the DRM-program itself could be also prevented by attesting the program by the trusted system.

Of course, virtually anyone can still search for new, unprotected content on the Internet. Joe may not be able to access the TCG-sealed Snow White file on his computer, but he can easily use a Peer-to-Peer file sharing program to find a different copy of Snow White in an unprotected file, which plays without a Disney-approved media program. This scenario doesn't implicate DMCA § 1201 because it deals with content not controlled by "a technological measure."[174] Although a very important digital copyright issue, because trusted computing does not presently prohibit users from *not using* the trusted system or DRM programs, the copyright implications of this scenario will not be discussed further in this paper.

2. Disaggregating Security from Digital Rights Restrictions

Disaggregation of trusted computing security from DRM restrictions poses challenges for DMCA § 1201 liability. DMCA § 1201(a)(1), individual anti-circumvention, likely applies to trusted systems in a similar fashion to present software-based DRM. A trusted computing security subsystem is plausibly a protected § 1201(a)(1) "technological measure." And, a trusted system could restrict access to a copyrighted work, satisfying the remaining elements of a DMCA § 1201(a)(1) anti-circumvention claim. Whether Joe hacks his software-based DRM program for his Snow White DVD, or hacks his TCG-compliant hardware to get at a trusted version of the Snow White file, he will likely be liable under § 1201(a)(1).

However, defending against individual cracks with DMCA § 1201(a)(1) isn't the real concern of the content industry. Copyright owners are far more concerned with the widespread distribution of tools that enable *all* of a DRM protection scheme to be broken.

[174] 17 U.S.C. § 1201.

The tools prohibited under DMCA § 1201(a)(2) (distribution of access-circumvention tools) and DMCA § 1201(b)(1) (distribution of copy-circumvention tools), if distributed worldwide, pose a threat to the security of all digital rights schemes.

Although previous sections in this paper indicate that any attacks beyond individual file cracks are technologically infeasible, the legal implications of a system-wide attack are still worth exploring. Assuming a tool capable of defeating trusted computing could be created and distributed, the implications for DMCA liability under § 1201(a)(2) and § 1201(b)(1) become more complicated. Both DMCA trafficking provisions create liability only where the device is primarily designed for circumvention, has limited commercial significance other than circumvention, or, is marketed as a circumvention device for cracking access or copy-protections.[175] In *Universal I*, the district court found that CSS effectively controlled copyrighted work, and that DeCSS was primarily designed to circumvent this access control under § 1201(a)(2)(A).[176] The court felt that this fact was enough to prove limited commercial significance as well.[177]

Trusted computing, by contrast, is not solely designed to protect a copyrighted work, as CSS does. Under one possible interpretation, distribution of a tool for *generally* cracking a trusted system would not necessarily create liability under DMCA § 1201(a)(2) or § 1201(b)(1), because there is no inherent primary design for such a tool. Cracking the one trusted computing scheme likely means cracking everything. Thus, a tool "solely" designed to crack Joe's Snow White DRM file, would be the same tool as one that allowed a forgetful end user to recover their own encrypted files or passwords on

[175] *See id*. § 1201(a)(2)(A)-(C); *see also id*. § 1201(b)(1)(A)-(C).
[176] *See* Reimerdes, 111 F. Supp. 2d at 318-19 ("... DeCSS was created solely for the purpose of decrypting CSS--that is all it does.").
[177] *Id*. at 319.

their computer. The DMCA makes a basic assumption that a technological protection measure will only have the purpose of protecting copyrighted works. When a technological protection measure like trusted computing has a more universal application (i.e., not just DRM), the liability model runs into ambiguous ground.

An alternate interpretation of the DMCA distribution provisions would argue that since a trusted subsystem "effectively controls access to a work" (or copying), any device which circumvents this protection scheme is liable under DMCA § 1201(a)(2) and § 1201(b)(1).[178] The argument would be that the trusted system effectively protects access and/or copy abilities for DRM programs, whether the protection is disaggregated from a DRM program or not. A general trusted system circumvention tool would thus be liable for cracking the entire trusted system security because the whole trusted system effectively controlled access / copy abilities for a DRM program. However, as described above, one has to hack the whole trusted system or none of it because the same protections are used, *regardless of function*.[179] DMCA liability in these scenarios could thus swallow the primary design requirement under § 1201(a)(2)(A) and § 1201(b)(1)(A) because the disaggregated trusted computing security model is not built with *any* primary design and any tool capable of circumventing trusted system-wide security is also capable of circumventing a DRM protection scheme relying on the same trusted system. This scenario ultimately raises a troubling prospect where DMCA anti-circumvention liability could be further extended to tools possessing no DRM circumvention purposes.

Additionally, the *implementation* or *marketing* of a specific trusted computing circumvention tool could still implicate DMCA liability. If a developer released a

[178] 17 U.S.C. § 1201(a)(3)(B); *see also id.* § 1201(b)(2)(B).
[179] Of course, this does not include individual hardware attacks on files as I am still referring to theoretical programs capable of circumventing the *whole* trusted subsystem.

program capable of cracking the entire trusted computing scheme, but which only actually implemented a specific DRM-cracking purpose, this would probably satisfy the primary design element of DMCA § 1201(a)(2)(A) or DMCA § 1201(b)(1)(A). And, a trusted computing circumvention tool (even if general in nature) marketed as a DRM-defeating device, would likely fall under DMCA § 1201(a)(2)(C) or DMCA § 1201(b)(1)(C), which creates liability for marketing a tool as a copyright circumvention device.[180]

3. Fair Use and the DMCA

The DMCA purports to respect traditional fair use in Section 1201(c)(1), declaring that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[181] Nonetheless, both the *Universal I* and *Universal II* courts upheld the proposition that fair use is not a defense to *anti-circumvention* liability for cracking access controls under the DMCA. Although possibly beyond the scope of Congress' intent for the DMCA, these are the only relevant rulings thus far.[182] Applied to a trusted computing DRM scenario, the fair use defense would be completely unavailable for cracking a trusted system, if a court found the trusted system a protected technological measure. Because the DeCSS courts allowed no fair use for cracking access controls, and cracking a trusted system for *any* purpose (even completely academic or traditionally fair use) requires cracking the whole system,

[180] *See* 17 U.S.C. § 1201(a)(2)(C); *see also id*. § 1201(b)(1)(C).
[181] *Id*. § 1201(c)(1).
[182] *See* Samuelson, *Digital Rights Management and/or/vs. the Law*, *supra* note 156 ("A careful study of the legislative history of the DMCA and the detailed structure of the anti-circumvention rules reveals that Congress intended for circumvention of copy- and use-controls to be lawful when done for non-infringing purposes, such as to enable fair uses.").

any trusted system circumvention tool would forego fair use defenses despite the optimistic statement in Section 1201(c)(1).

4. DMCA Statutory Exceptions

The DMCA contains several statutory exceptions. Considering the narrow language of the provisions, none are likely to create significant immunities for the dissection of a trusted computing system. Nonetheless, these provisions are likely to come to the forefront of the DRM debate once trusted computing systems become more prevalent.

a. Reverse Engineering and Protecting Proprietary File Formats

DMCA § 1201(f) provides a circumvention exemption for reverse engineering. Section 1201(f)(3) requires that the exempted circumvention be "solely for the purpose of enabling interoperability" with other programs. In *Universal I*, the district court held that DeCSS did not qualify for a reverse engineering exception because DeCSS did not "solely" enable interoperability of DVD's with the Linux operating system - the program also worked on Windows.[183]

However, this exemption could prove important to software developers working with trusted computing systems. Because trusted computing can encrypt and seal files from any program with ease, software developers could use this functionality to ensure that *only* their programs could use their proprietary file formats. A common worry is that Microsoft will utilize trusted computing to ensure that Word documents can only be

[183] *See* Reimerdes, 111 F. Supp. 2d at 319-20.

opened with the Microsoft Word.[184] Microsoft has already announced that digital rights management will be built into its Office 2003 software, and will possibly thwart compatibility with other word processing programs and previous versions of Microsoft products.[185] When trusted computing becomes available, such a scheme will be even more effective.

Trusted computing threatens to change the whole arena of reverse engineering. The open source community relies extensively on such reverse engineering of proprietary protocols and document formats in general to produce open source software.[186] Critics already pose that the DMCA's restriction of acceptable reverse engineering is overbroad and gives too much legal protection to content owners.[187] Trusted computing could augment content owners' technological protection of proprietary formats. To successfully create an interoperable product, the *whole* system must be cracked. If Company X wants to create a legal alternative viewing program for Joe's Snow White digital file, it must rely on being able to play *all* digital files from Disney, not just Joe's. Thus, if trusted computing security is resistant to such a system-wide attack as promised, then the legal status of reverse engineering is a needless investigation - reverse engineering will be technologically impossible.

---

[184] *See* Stallman, *Can You Trust Your Computer?*, *supra* note 4 ("Word processors such as Microsoft Word could use treacherous computing when they save your documents, to make sure no competing word processors can read them. Today we must figure out the secrets of Word format by laborious experiments in order to make free word processors read Word documents. If Word encrypts documents using treacherous computing when saving them, the free software community won't have a chance of developing software to read them--and if we could, such programs might even be forbidden by the Digital Millennium Copyright Act.").

[185] David Becker, *New Office Locks Down Documents*, CNET News.com (Sept. 2, 2003), *at* http://news.com.com/2100-1012_3-5069246.html (last visited Dec. 26, 2003).

[186] *See* Stallman, *Can You Trust Your Computer?*, *supra* note 4.

[187] For an in-depth discussion of the issue of reverse engineering and the implications of the DMCA, *see* Pamela Samuelson et al., *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575 (May, 2002) [hereinafter Samuelson, *The Law and Economics of Reverse Engineering*].

If, on the other hand, the entire trusted computing system could be compromised, then DMCA anti-circumvention liability is still a possibility. To invoke Section 1201(f) as a defense to anti-circumvention liability for their work, reverse engineers would have to be very careful. The security to the trusted computing subsystem is disaggregated, but Section 1201(f)(3) requires that the *only* purpose of reverse engineering be interoperability with another program. Thus, at least under the *Universal I* analysis, an interoperable program would have to crack the whole trusted computing system, and then implement the narrowest set of functionality that would only enable an end user to interoperate with the program. Essentially, if Company X made a Linux viewing program for Joe's Snow White video, in order to escape anti-circumvention liability with DMCA § 1201(f) they would have to ensure that program only worked on Linux and that it did not disable any of Disney's DRM controls.

b. Protecting Personally Identifying Information

Trusted computing systems must contain personally identifying information for attestation functions, so that third parties can determine which end user is requesting digital content. The use of digital personal information has already garnered a firestorm of controversy from privacy advocates.[188] Keeping digital privacy in mind, DMCA § 1201(i) allows individual end users to circumvent access controls solely to protect personally identifying information.[189] However, the exemption is of very limited significance to cracking a trusted computing security scheme. The exception applies only to individual users and not to the distribution of circumvention tools. And, although

[188] *See, e.g.*, Cohen, *DRM and Privacy*, *supra* note 169.
[189] 17 U.S.C. § 1201(i).

individually cracking a trusted computing-protected file is possible, the end user is only allowed to remove personally identifying information under the DMCA § 1201(i) exemption. Such a change to the file would almost certainly render the digital file untrusted by the system and it would fail in any remote attestation exchange. Joe could possibly crack his Snow White file and remove the identifier "Joe Smith" from the file, but doing so would make the file unplayable, and Disney would likely not re-approve the file for Joe's use without personally identifying him. Thus, although DMCA § 1201(i) applies in theory, it would be of little practical use for privacy-minded members of the public.

c. Security Testing and Encryption Research

The DMCA exceptions for security testing and encryption research give some leeway to researchers and security experts attempting to crack a trusted computing scheme.[190] The DMCA's encryption research exemption, Section 1201(g), requires that the conduct be "necessary to conduct such encryption research"[191] and for the purpose of disseminating information "to advance the state of knowledge" rather than providing a practical exploit.[192] The security testing exemption, Section 1201(j), applies only to persons testing their own internal computer security and prohibits dissemination in any manner that facilitates copyright infringement.[193] Essentially, these exemptions allow purely informational / academic dissection of a trusted computing security platform. But,

[190] *See id.* § 1201(j); *see also id.* § 1201(g).
[191] *Id.* § 1201(g)(2)(D).
[192] *Id.* § 1201(g)(3)(A).
[193] *See id.* § 1201(j).

the limitations on both exemptions prevent any workable circumvention of a trusted computing scheme to escape liability using Section 1201(g) or Section 1201(j).

The DMCA was Congress' answer to the demands placed upon copyright by the digital revolution. However, it appears that just years later, the rapid pace of technological development is straining even the newest legislation. Trusted computing security models challenge the DMCA because it wasn't designed with disaggregated security and protection measures in mind. To the further chagrin of DMCA critics, anti-circumvention liability could possibly expand under trusted computing-backed DRM schemes. Or, the general application of trusted computing could immunize some forms of circumventing conduct. Finally, differing possible interpretations of liability may be wholly unnecessary, for if trusted computing effectively locks out *all* system-level hacking, then the content owner's technology will trump the application of copyright law.

B. Building Blocks in the Pursuit of "Private" Copyright Law

Evolving DRM schemes raise the specter of the "privatization" of copyright law by content owners, where technology and not the law governs copyrights. Although traditional copyright law has many exemptions and limitations, DRM with trusted computing offers the possibility of *absolute* control over the public's use of digital content. Content owners clearly have a vested interest in policing copyright infringement with technologies that they can control, in lieu of legal remedies that they often cannot.

Many critics argue that such a privatization by DRM threatens the public's copyright rights and freedoms. Robin Gross notes that

> [b]y essentially privatizing copyright law, these DRM schemes maintain none of the balance that the public law of copyright enshrines. Ironically, society is embarking on a dangerous path of narrowing the public's access to creative expression at exactly the time that technological advances protect publishers' rights more effectively than ever before.[194]

Professor Elizabeth Thornburg poses that absolute DRM schemes threaten to entirely control public copyright principles such as fair use, first sale rights, and making backup copies - each specific use would have to be licensed from the content owners.[195] Thornburg contends that digital copyright controls are particularly problematic because there is no external, human check on the restrictions of DRM systems.[196] Essentially, DRM systems create the equivalent of a permanent injunction against traditional copyright exemptions with significant procedural biases in favor of the content industry.[197] Professor Lawrence Lessig questions the public's recourse under such a scenario and postulates that

> the problems are worse when code displaces copyright law. Again -- where do we challenge code? When the software protects in a particular way without relying in the end on the state, where can we challenge the nature of the protection? Where can we demand balance when the code takes it away?[198]

---

[194] Robin Gross, *Copyright Zealotry in a Digital World: Can Freedom of Speech Survive?*, *in* COPY FIGHTS 190-91 (Adam Thierer & Wayne Crews eds., 2002).

[195] Thornburg, *Going Private*, *supra* note 4, at 176 ("Trusted system enthusiasts note that they provide for greater control than copyright law; the DRM, rather than copyright law, controls the use of the product. For example, the creators of trusted systems anticipate that fair use of copyrighted material must be purchased with a license. So would first sale rights: the right to read, watch, or listen to a work would be licensed separately from the right to read it again, copy it, print it, or whatever. So would the right to make a backup copy. Each use would be licensed and charged an associated fee.").

[196] *See id*. at 190 ("There is no complaint, no response and no dispute resolution provider. There is certainly no court involvement in determining the remedy. There is not even a human involved in invoking the DRM.").

[197] *See id*. at 195 ("The DRMs eliminate the need for an injunction and completely reverse the parties' procedural posture. One type of DRM prevents the licensee from engaging in an unauthorized use (or charges fees for expanded use, as if it were an award of damages measured by a license fee). This is the equivalent of a permanent injunction against the expanded use."); *see also id*. at 196 ("The DRMs arguably provide the starkest shift of procedural advantage. The licensor does not even have to file a complaint, much less prove an entitlement to an injunction from a balance of the equities.").

[198] Lessig, CODE, *supra* note 4, at 136.

Because of the fallibility of existing software-based DRM schemes, the public has yet to grapple with any serious DRM impediments. Trusted computing may well take a large role in changing this. The low level security schemes inherent in trusted computing will present very effective protection mechanisms for DRM programs, at least for the near term. And, there are no technological mechanisms for fair use or other copyright limitations built into current trusted computing specifications. Content owners and DRM producers will likely be able to specify *exactly* what the public can or cannot do with their content. When trusted computers actually ship and DRM producers write programs on top of trusted platforms, technology will possibly hand over all control of digital copyright law from the legal system to the content industry.

C. The Emerging Digital Rights Management Arms Race

The new level of DRM security possible with trusted computing is not likely to last over the long term. Trusted systems don't address the fundamental problem posed by security experts - one *cannot* ultimately control bits of information on the public's computers. As previously noted, trusted systems explicitly do not protect against specific hardware attacks. Thus, the Napsterization threat model remains open and trusted computing will fail as a security framework for DRM because of development of system-wide exploits or the distribution of single, cracked files over the Internet. The content industry will then have to look to a new technology that promises to finally, finally lock down all of the bits on a user's system. However, if Schneier and his compatriots are correct, even this next technology won't be completely secure because it is impossible to secure *all* computers, and the cycle will continue.

Most likely, the public will be left in an "arms race" scenario, where the content industry continually pursues new technologies for DRM systems that clever hackers will inevitably manage to break, preventing a completely secure system. Professors Pamela Samuelson and Suzanne Scotchmer note that such a "measures-and-countermeasures war" is likely to be expensive and wasteful.[199] They also observe that such a "war" is driven in part by DMCA anti-circumvention liability, which gives significant advantages to the content industry.[200] Nonetheless, despite the specter of DMCA liability and improved technology, hackers and reverse engineers appear determined to release circumvention tools.

The public stands to lose both traditional copyright freedoms and improved technological functionality in such a conflict scenario. Most of the public will likely to be unable to circumvent trusted computing-based DRM. And, they will be less likely to circumvent the subsequent DRM systems. However, as the content industry and DRM developers tirelessly work on thwarting the hacker elite, resulting DRM systems will become more and more restrictive. Mark Cooper, research director for Consumer Federation of America observes that DRM "isn't going to stop serious hackers" - "[a]ll you end up with here is an inconvenience to the average consumer."[201] Trusted systems will no longer allow the public access to their own digital files. Perhaps this is an acceptable cost, given the personal security benefits of trusted computing. But, a substantial issue remains - what will the next generation of DRM systems force the public to give up?

---

[199] Samuelson, *The Law and Economics of Reverse Engineering*, *supra* note 187, at 1641.
[200] *See id.*
[201] Harmon, *Digital Armor*, *supra* note 34.

D. The Future of Digital Copyright Controls and Winning the Arms Race

The content industry cannot solve the Napsterization threat model by solely relying on trusted computing to stop copyright infringement. Already, there are signs that perhaps the content industry is ready to embrace a casual-copying threat model, focusing only on keeping the majority of the public honest. Apple Computer's iTunes Music Store appears to be a step in this direction.[202] Apple's downloadable music files are protected by DRM that allows end users wide latitude in the copying and use of digital files. The combination of reasonable pricing ($1 per song) and a modest DRM scheme appears popular - Apple has sold over 3 million songs since the Music Store's launch.[203]

In the alternate, the most logical push by the content industry in the future will be to contain the damage of single file cracks by preventing their use on other machines. However, for that to happen, virtually all unprotected digital content must be regulated - an extraordinarily substantial task. This would most likely mean technological or legal mandates.[204]

If trusted computing becomes technologically ubiquitous, a DRM system can be superimposed on the framework. Technology companies could then pursue DRM operating systems (like that in Microsoft's DRM OS patent) that freeze out any unprotected content. If enough people can be enticed to purchase computers that

---

[202] *See* Borland, *Apple Unveils Music Store*, *supra* note 46.
[203] *See* Evan Hansen, *Amazon vs. Apple in Music Downloads?* , CNET News.com (May 29, 2003), *at* http://news.com.com/2100-1027-1011293.html ("Since its April 28 launch, Apple's iTunes Music Store has sold 3 million songs. iTunes charges 99 cents for singles and $9.99 for full albums. The pace of sales has slowed to about 100,000 tracks a day, about half of its opening-day volume. ").
[204] Samuelson, *Digital Rights Management and/or/vs. the Law*, *supra* note 156 (observing that "DRM can be mandated in two ways: through standard-setting processes or through public legislation" and detailing the current technological and political candidates for such mandates).

technologically restrict any unauthorized digital copyright use, then perhaps DRM does have a chance at solving the break-once, break-everywhere problem. Unfortunately, it remains rather difficult to convince the public to buy into a technology that substantially restricts functionality and freedom.

On the legal side, Senator Holling's CBDTPA would mandate that effective DRM be built in to every new computing device. Such a law would likely solve break-once, break-everywhere problem of DRM because each individual computer would only play authorized content. Each CBDTPA computer would need to be individually cracked to play unauthorized content. But *requiring* that every computer restrict a wide range of digital conduct is an enormous leap from the more modest fact of trusted computing *offering* tools to implement DRM functionality. Thus, for the time being, it appears that the technology industry, the civil libertarians and political opponents of DRM mandates will keep such legislation at bay.

Many parties have also offered solutions to sway the balance of power away from the content owners. The Boucher, Wyden and Lofgren bills all attempt to chisel away at the legal side of content industry's DRM campaign. Hackers, like Jon Johansen, chip away at the technology each new DRM protection scheme. From both ends, Deidre Mulligan and Aaron Burstein argue that perhaps copyright limitations can be built in to DRM languages and implementations.[205] Dan Burk and Julie Cohen suggest that

[205] *See* Deirdre Mulligan et al., *Implementing Copyright Limitations in Rights Expression Languages* (Nov. 18, 2002) (posing that if digital rights management languages "are to be agnostic as to legal context they must at least support the expression of the exceptions and limits on exclusivity found in copyright policy" and that such copyright exceptions should be implemented in the technical rights languages), *available at* http://crypto.stanford.edu/DRM2002/mulligan_burstein_acm_drm_2002.doc (last visited Jan. 6, 2004).

additional technology and/or regulation can regain traditional fair use grounds under developing rights management schemes.[206]

And, perhaps an "arms race" in trusted computing or DRM development isn't such a bad thing after all. The astonishing rate of development of technologies is likely due in large part to the various parties, problems, incentives and pressures surrounding the changing technological arena. Adam Thierer, an analyst for the Cato Institute, poses that for DRM:

> [t]he better alternative to federal mandates on either side of this debate is to instead just encourage a technological free-for-all in the marketplace[.] Let the industry do whatever it wants in an attempt to bottle up their content, but also let consumers continue to experiment with and use digital content in creative ways without fears of federal intervention at every turn... There's no reason for Congress to intervene in an attempt to solve each and every intellectual property dispute, as has seemingly becoming the case in recent years.[207]

Conclusion

Trusted computing is a complex technical subject as well as a complicated policy issue for digital copyright law. Digital rights management will continually be pursued by the content industry in the attempt to plug the holes created by Napster and file sharing on the Internet. Trusted computing offers a new level of security for computers with both negative and positive implications for the public. Developers point out that trusted computing systems are agnostic towards DRM. But the DRM implementations built on trusted systems will not be. Trusted computing will provide a building block for a new

[206] *See* Dan Burk & Julie Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001).
[207] McCullagh, *Senator Calls For Copy-Protection Tags*, *supra* note 67 (quoting Thierer).

generation of secure DRM technologies, but is not the ultimate problem nor final solution for the DRM debate. At least not yet.

For the near term, the new model of disaggregating security features from DRM functionality creates issues for the inevitable DMCA anti-circumvention debate once hackers set in to defeat trusted computing devices. Trusted computing will provide the means for another step towards that privatization of digital copyright law. And, the range of the public's traditional copyright freedoms will incrementally narrow, with expanding legal doctrines on one side, and stronger digital rights locks on the other.

Over time, DRM based on trusted computing cannot lock down all computers without the help from either legal or economic forces. The content industry will continue to push for stronger legal and technological DRM measures, which hackers will attempt to break, while civil libertarians voice their concerns. The technology community is still split over the content industry's demand for secure DRM technologies and the public's insatiable appetite for devices without such controls. And, predictably, the politicians are listening and responsive to all parties on the issue. But, from any perspective, trusted computing demonstrates that as the stakes are raised in the DRM controversy, the public risks being left in the middle of an ever-escalating war for copyright control on their computers.