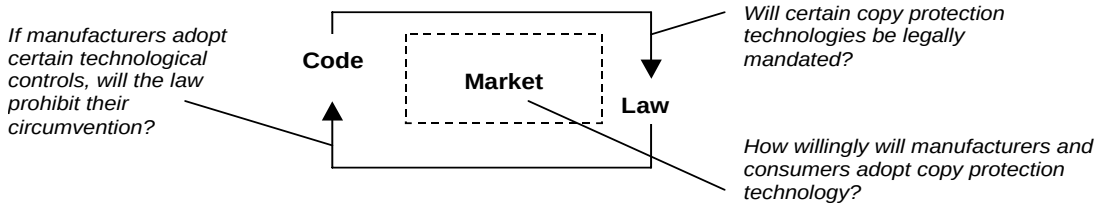
Chapter 9

Technological Counterparts to Copyright

Chapter Overview

Those who have sought to protect access to and use of their content on the Internet began with a basic legal strategy. As chapters <X> explain, expansion of the substantive scope and practical enforcement of intellectual property laws has been an important tool in the publishers' defensive toolkit. Early use of the law to prevent copying of publishers' content accepted the state of the Internet – and the abilities it affords its users to move data around quickly, cheaply, and accurately – as a fact of nature, its abuses perhaps to be railed (and legislated) against, but itself not fundamentally altered

The failure of a legal approach to solve the publishers' problem – indeed, the emergence of copyrighted file swapping as a mainstream use of the Internet – has led publishers to embrace a much more sophisticated approach to containment. This approach centers on technological changes to the Internet and the machines connected to it, re-engineering what was too quickly conceded to be that fact of nature. The general idea is to create technological shields for digital assets: architectural limits on how particular data can and cannot be used by end-users. Such shields may offer a faster, cheaper and more reliable way of regulating access to online information than does the law, and in theory could harness networked technologies to simply better approximate the state of affairs before the Internet came about – or even afford greater control over content and its uses than law alone could ever attempt.



To be sure, technological shields have abundant, perhaps inherent, limitations. They are arms within a classic arms race; each new generation of protective technologies has spawned efforts to overcome or circumvent these controls. As the locks get better, so, too, do some of the lock-pickers.

The Internet's usefulness as a resource to develop, promote and distribute circumvention technologies greatly exacerbates this phenomenon. Thanks to the Net, those who labor to circumvent technological controls can coordinate efforts, share information and promote and distribute their successes.

Another problem with technological shields lies within the claim that a chain is only as strong as its weakest link. Securing digital assets is extremely difficult given the diverse range of platforms upon which digital content may be deployed. Security measures deployed in DVD technology, for example, might render content relatively secure when played on DVD players, yet that same technology might offer less control when the DVD is accessed by a personal computer. Developers of technological controls face the often daunting task of securing content on every imaginable platform, and coordinating with each other – across typically competitive company lines – to do so. This is especially important when – as is most often the case – content compromised on any one platform can be easily reproduced without technological controls in a form deployable on all platforms.

In the face of these challenges, even the most ardent evangelists of a technological approach to content control allow that the law can operate to bolster technological controls. This can be accomplished by penalizing (criminally or otherwise) circumvention efforts, or perhaps by governments' mandating manufacturer compliance with technological regimes that enable the deployment of private controls. The first approach aims to deter circumvention by giving technological controls the weight of the law. The second approach aims to solve the "weak link" problem by imposing industry-wide security standards reflected within machine hardware as well as software. We consider both types of initiatives in this chapter.

Critics of a strategy to legislatively support architectural changes to cyberspace for the purposes of limiting copying have raised a variety of ideological objections. Among these objections lies a fear that this type of legislation will stifle technological innovation and research. Opponents also argue that this approach will enable content providers to create and assert "rights" through software that are otherwise not found in law – or at least were not so protected before the law itself was changed to conform precisely to such technological barriers, wherever they might be built.

Protective technologies: An introduction to encryption and trusted systems

A. Encryption

Please see Section <X> of <X> (Supplement?, Appendix?, web?), "The Basics of Encryption."

B. Trusted Systems

1. What are trusted systems?

Perhaps the most important example of efforts to deploy technological shields to protect content is the development of so-called "trusted systems."

Jonathan Zittrain
What the Publisher Can Teach the Patient: Property and Privacy in an Era of Trusted Privication
52 Stanford L. Rev. 1201 (2000)

> The music industry until recently feared ruin from the unauthorized swapping and rebroadcasting of high-quality audio reproductions among its customers, a phenomenon enabled by increasingly cheap networks, cheap data storage, and cheap processors - … the Era of Promiscuous Publication. Despite access to a sympathetic Congress and extensive enforcement resources, the music industry has found recourse to law largely unavailing against this tide of technological progress. The industry is now embarking on a different strategy - changing the technology itself. At the core of the technological response lies the idea of "trusted systems": computer databases of the rights and privileges of specific entities vis-à-vis information, linked to hardware and software that recognize and enforce those rights. If fully deployed, trusted systems could trump the Era of Promiscuous Publication with what I call an "Era of Trusted Privication": one in which a well-enforced technical rights architecture would enable the distribution of information to a large audience – publication - while simultaneously, and according to rules generated by the controller of the information, not releasing it freely into general circulation - privication.
>
> ...
>
> Within the past five years, a new strategy has come to the fore to deal with the impact upon information sharing (or, from the point of view of those who wish control, "piracy") by cheap processors, networks, and storage-a strategy quite different from the incrementalism of tighter enforcement of substantively stricter rights, whether through public law or private contract. The strategy is ambitious, with a fantastic payoff of control to publishers generally, and the music industry specifically, if it can be accomplished.
>
> The premise is simple: the Net of today is what we have made it - and the Net of tomorrow will be however we remake it. Each need not bear much resemblance to the other. Publishing executives who think that the unfortunate ease of information flow is an inherent quality of the Internet - indeed, a necessarily ever-accelerating one - suffer from "is-ism." So do neo-libertarians who think that the Net's current unsuitability to regulation is simply a fact of life to be celebrated rather than an architectural decision that once made may still require sustained practical if not theoretical defense. The cliché that the Internet "recognizes censorship [and presumably information blockage from any source] as damage and routes around it" has perhaps prematurely achieved the stature of truism.
>
> How could a future Internet realistically tame the current information chaos? Mark Stefik, a researcher at Xerox PARC, has been quietly developing and touting an answer for several

years. Stefik is among the leading architects of so-called "trusted systems," technological gatekeepers that allow "authorized" flows of information while flatly blocking "unauthorized" uses. A necessary element is the ability to structure "rights" into a calculable framework that is then automatically enforced by the technology, whether the user pleases or not. To the extent that these rights architectures are made secure - when, through a combination of hardware and software, a user who is anything less than a talented hacker is truly constrained by the system at the behest of whoever is the source of the information it might display - the system can be said to have "trust." A trusted system is one that can be trusted by a rights-holder as against the user of the system - even if the physical system is in the custody of the user. ...

Multi-user operating systems have long had rudimentary "rights" architectures. Files have "owners." Owners can specify who else on the system can view the file. They can independently specify who else on the system can alter the file-indeed, some might be permitted to view the file without altering it, while others might be permitted to alter the file without viewing it. Owners can even alienate the right to assign new rights: a simple command transfers ownership to another user. In more sophisticated systems, "audit trails" reveal to the owner (or to proxies to whom the owner has delegated the relevant right) who among those authorized has peeked at a file and when.

Thus, a trusted system might include a vernacular through which a publisher could tag a document as "not to be copied, in whole or in part." A consumer could be sent the document - put more precisely, might have "read access" to it - but upon attempting to highlight a portion, copy it, and paste it elsewhere - perhaps in an email to send to a friend - would receive an admonition from the computer that says "operation not allowed." Or a publisher might label the document with a fifty-cent printing fee, and upon asking for a printout the consumer would, in turn, be asked by her computer to pay fifty cents. No payment, no printout.

Further, tying nuanced forms of access to information to one's identity or characteristics enables highly targeted price discrimination. One could give access to a text at "retail" price to a businessperson and at a discount to a student; one could let certified Democrats see something that Republicans (or at least non-Democrats) could not.

The music industry, then, should refrain from utter despair about piracy - and there are signs that it is doing just that. Trusted systems comprising computers linked by cheap, fast (perhaps wireless) networks could enable the following hypothetical world of commercial music:

Songs are not "sold" in even the colloquial sense of the word; rather, they are "licensed" - both from a legal and technical standpoint. Compact discs have joined 8-tracks, cassettes, and phonograph records in the dustbin; their replacements are small, generic "jukeboxes" linked by the Net to a central repository of songs managed by a publisher.

An individual authenticates herself to a jukebox - perhaps with a fingerprint or carefully scrawled signature on its back with a stylus - and then may access specific songs that fall under her monthly payment plan. She will be granted access to the music archive only after parting with personal information about herself, including name, age, address, and phone number. (This information is passed in a heartbeat to the publisher from her personal computer's registration module; she entered and authenticated it once, and it is now requested constantly as she uses the computer to visit various web sites. She has long since set her "preferences" to release it if access to the site will be denied otherwise.)

As she selects songs, her tastes are noted, allowing offers for "special" songs not included in her monthly plan to be specifically targeted to her tastes and sent to her across all media. The songs she asks for are "streamed" to her player as she listens, and do not remain there any more than a song stays inside a radio after it is over.

An inaudible signal is embedded in the music; if she holds a microphone to her headphones and thereby makes an imperfect, analog copy to an old-fashioned cassette, her name

and a unique identifier will be "in" it, permitting prosecution for copyright infringement if the copy is found. Her user license agreement provides an alternative path for the music owner to pursue fast-track damages, including the sending of a signal to her jukebox that permanently disables anyone from using it until the matter is settled.

In the unlikely event that she were to abuse her access to the system by hooking up her jukebox to an amplifier and playing the music at a backyard party outside her California apartment, a cheap listening post on the beach's lifeguard chair could be monitored by ASCAP, which would use a watermark decoder to know instantly that she was behind the cacophony - and that the particular performance had only been paid for at the "portable personal use" rate rather than the "noncommercial party" rate. (Music data from listening posts might be shared with ASCAP by the local police department, which has deployed a network of microphones around the city to respond to the sound of gunshots in the area.)

A more likely event is that she will fall behind in her monthly payments, in which case her access to any music - except that which is heard over old-fashioned analog "public" radios - will be cut off automatically. (This may soon happen; her monthly rate just doubled since her graduation from college and corresponding loss of student discount status.)

A world like this is still at least five years off by my conservative reckoning - and the music industry may, after consulting its own muses and the market, elect not to invoke all the technical power that could be at its disposal. Still, publishing industries have already taken the first halting steps towards trusted systems architectures.

…

To be sure, these steps are merely beginnings, and they include as many failures as successes. However, there are reasons why the music industry appears to be placing its faith in technology, knowing full well that the industry's interests cannot be assumed to be identical to those of the hardware and software vendors who would have to support trusted technology, and that a number of independent creative minds will be bent on breaking any locks it might convince the institutional technologists to come up with.

At least one formal process has at last coalesced through which a new generation of computer hardware can augment the software of "trust," demonstrating cooperation between content providers and consumer systems architects, and posing a new kind of challenge to those who would seek to crack the code. The Trusted Computing Platform Alliance was formed to little fanfare in October 1999, by the most powerful companies in information technology:

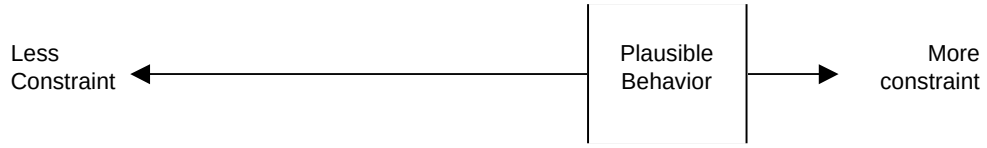
The Trusted Computing Platform Alliance, or TCPA, was formed by Compaq, HP, IBM, Intel and Microsoft. All five companies have been individually working on improving the trust available within the PC for years. These companies came to an important conclusion: the level, or "amount", of trust they were able to deliver to their customers, and upon which a great deal of the information revolution depended, needed to be increased and security solutions for PC's needed to be easy to deploy, use and manage. An open alliance was formed to work on creating a new computing platform for the next century that will provide for improved trust in the PC platform.

Where before a simple illicit software patch might break a particular protection scheme, the TCPA's work could ensure that a computer owner might have to take a soldering iron to the computer's circuit board in order to circumvent a protection scheme, significantly raising the costs of quick and perfect copying to rival those of the monastic manuscript era.

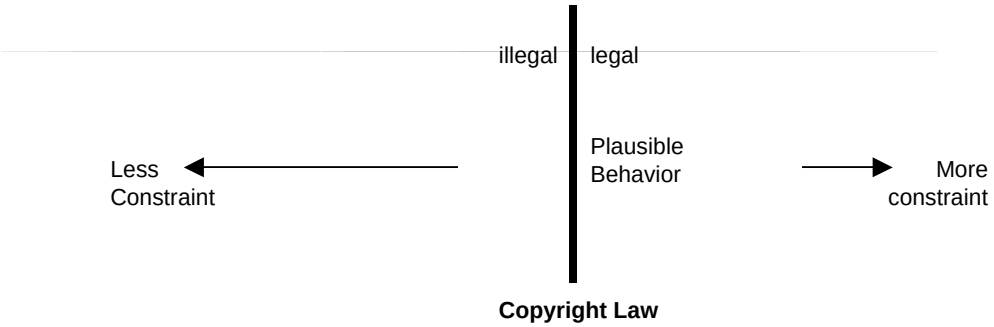
The ambition of this technical strategy in response to the panic over the Internet free-for-all is to hasten a new era (or perhaps take us back to an earlier one) before the current one has truly settled in. We might revise Post's recounted timetable as follows:

- Era of Monastic Manuscript: Copyright unnecessary to authors or publishers
- Era of Gutenberg Press: Copyright necessary to authors and publishers
- Era of Promiscuous Publication: Copyright enforcement doubtful.
- Era of Trusted Privication: Copyright unnecessary to authors or publishers.

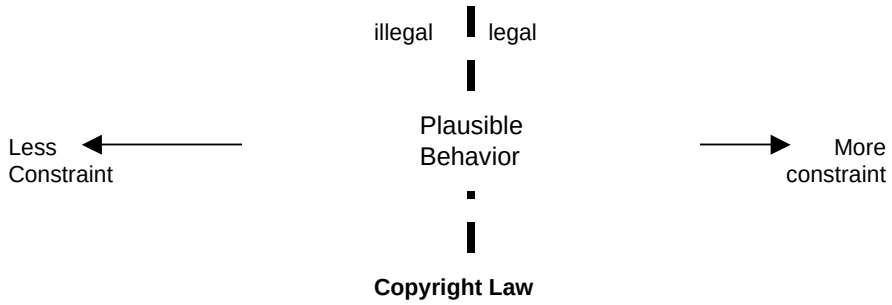
1) *Era of Monastic Manuscript:* Copyright law is unnecessary because it's so hard to make copies in the first place.



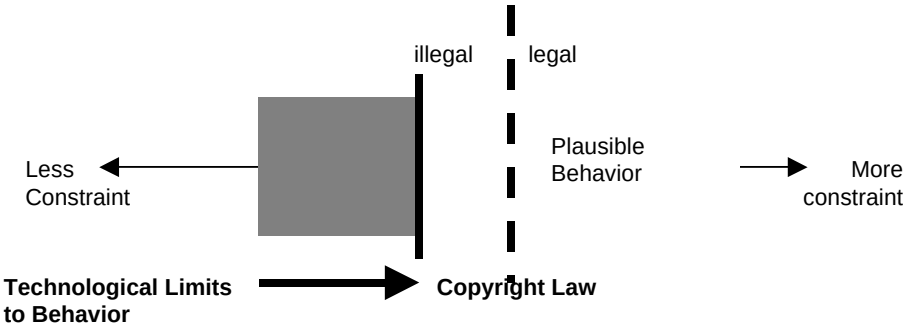
2) *Era of Gutenberg Press:* Copyright law becomes necessary as the printing press enlarges the scope of plausible behavior.



3) *Era of Promiscuous Publication:* Copyright Law becomes difficult to enforce, and the Internet enlarges the scope of possible behavior even further.



4) *Era of Trusted Privication:* Technology complements copyright by limiting behavior which is hard to regulate otherwise.



The term "privication" is meant to capture the heretofore-unlikely coupling of mass distribution of information to "authorized" users with tight control over its use-at least along the dimensions of perfect, instantaneous, and anonymous copying. That control is enabled through private rather than public means, eliminating the need for copyright to the extent that the trusted system can be relied upon to protect information.

Mark Stefik

Trusted Systems

Scientific American, March 1997.

Everyday experience with computers has led many people to believe that anything digital is ripe for copying—computer programs, digital books, newspapers, music and video. Some digital-age pundits have gone so far as to proclaim that the ease of duplicating data heralds an end to copyright: information "wants to be free," they assert. It is impossible to thwart the spread of information, so the argument goes. Anything that can be reduced to bits can be copied.

…

Behind the scenes, however, technology is altering the balance again. Over the past few years, several companies, including Folio, IBM, Intertrust, Net-Rights, Xerox and Wave Systems, have developed software and hardware that enable a publisher to specify terms and conditions for digital works and to control how they can be used. Some legal scholars believe the change is so dramatic that publishers will be left with too much power, undercutting the rights and needs of consumers and librarians.

…

The key to this technological shift is the development of what computer scientists know as trusted systems: hardware and software that can be relied on to follow certain rules. Those rules, called usage rights, specify the cost and a series of terms and conditions under which a digital work can be used. A trusted computer, for instance, would refuse to make unauthorized copies or to play audio or video selections for a user who has not paid for them.

Trusted systems can take different forms, such as trusted readers for viewing digital books, trusted players for playing audio and video recordings, trusted printers for making copies that contain labels ("watermarks") that denote copyright status, and trusted servers that sell digital works on the Internet. Although the techniques that render a system trustworthy are complex, the result is simple. Publishers can distribute their work—in encrypted form—in such a way that it can be displayed or printed only by trusted machines. …

How does a trusted system know what the rules are? At Xerox and elsewhere, researchers have attempted to express the fees and conditions associated with any particular work in a formal language that can be precisely interpreted by trusted systems. Such a usage-rights language is essential to electronic commerce: the range of things that people can or cannot do must be made explicit so that buyers and sellers can negotiate and come to agreements. Digital rights fall into several natural categories. Transport rights include permission to copy, transfer or loan. Render rights allow for playing and printing. Derivative-work rights include extracting and editing information and embedding it in other publications. Other rights govern the making and restoring of backup copies.

How Trusted Systems Work

Different intellectual works have different security requirements. But trusted systems allow publishers to specify the required security level to safeguard a document or video. The most valuable digital properties might be protected by systems that detect any tampering, set off alarms and erase the information inside. At an intermediate level, a trusted system would

block a nonexpert attack with a simple password scheme. And at a lower security level, it would offer few obstacles to infringers but would mark digital works so that their source could be traced (such digital watermarking is now embedded in some image-manipulation software).

Most trusted computers have the capability to recognize another trusted system, to execute usage rights and to render works so that they either cannot be copied exactly or else carry with them a signature of their origin. For executing a highly secure transaction, two trusted systems exchange data over a communications channel, such as the Internet, providing assurances about their true identities. Managing communications over a secure channel can be accomplished with encryption and what are known as challenge-response protocols.

…

Trusted systems can place identifying watermarks that make it possible to track down unauthorized duplications or alterations. Watermarks maintain a record of each work, the name of the purchaser and a code for the devices on which they are being played. This information can be hidden—in the white space and gray shades of a text image, for instance. As such, the identifying information would be essentially invisible to lawful consumers—and unremovable by would-be infringers.

Publishers would still need to be watchful for unlicensed distribution of their property. A computer user can always print a digital page and then photocopy it. A digital-movie pirate can sit in front of the screen with a camcorder. What trusted systems prevent, however, is the wholesale copying and distribution of perfect digital originals. With appropriate watermarks, for instance, even pirated copies should still be traceable.

Notes and Questions

1) Suppose a book were printed on individual pages that, after ten minutes' exposure to light, would turn brown and become unreadable. Would the market for the book differ from that of a regular book? Would some types of books be better suited to such marketing than others? How much would it matter that some readers might buy infrared flashlights and goggles and read the books in the dark? Retype them into a computer?

2) A friend sends you a small program by email that, when clicked upon, promises to illicitly register the unlicensed copy of a word processor that you've installed on your computer. What are your most convincing reasons to use it? Not to use it?

3) Suppose a music CD you order by mail, at a heavy discount, is pressed specifically for you: it sounds like any other to the human ear, but its music contains an inaudible background "watermark" that identifies you as the purchaser. The CD is clearly labeled with a warning: Should a copy of a song from that specific disc find its way onto the internet, the music publisher who found a copy would be able to trace it back to you. Would this make you any less likely to buy the CD? Accept it from the company as a free promotion? Share it on the Internet?

2. The Prospects of Industry Support for Trusted Computing Architectures

If systems like Stefik's are to come about, the major producers of software and perhaps hardware will have to build them. What reasons might they have for wanting to do so, especially if piracy-resistant products are of less use to the consumers who buy them? (Recall the Sony case, *Sony v. Universal Studios*, 464 U.S. 417 (1984), supra <X> – there Sony, a manufacturer of VCR's, was intent on preventing publishers from restricting their use and distribution.) This section offers some insight into the interplay between publishers and consumer device and software manufacturers, tracing an increasing alignment of goals from the times when one was suing the other.

From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: Microsoft and Subsidiaries: All [Full-Time Employees]
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing — or able — to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

When we started work on Microsoft .NET more than two years ago, we set a new direction for the company — and articulated a new way to think about our software. Rather than developing standalone applications and Web sites, today we're moving towards smart clients with rich user interfaces interacting with Web services. We're driving the XML Web services standards so that systems from all vendors can share information, while working to make Windows the best client and server for this new era.

There is a lot of excitement about what this architecture makes possible. It allows the dreams about e-business that have been hyped over the last few years to become a reality. It enables people to collaborate in new ways, including how they read, communicate, share annotations, analyze information and meet.

However, even more important than any of these new capabilities is the fact that it is designed from the ground up to deliver Trustworthy Computing. What I mean by this is that customers will always be able to rely on these systems to be available and to secure their information. Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony.

Today, in the developed world, we do not worry about electricity and water services being available. With telephony, we rely both on its availability and its security for conducting highly confidential business transactions without worrying that information about who we call or what we say will be compromised. Computing falls well short of this, ranging from the individual user who isn't willing to add a new application because it might destabilize their system, to a corporation that moves slowly to embrace e-business because today's platforms don't make the grade.

The events of last year — from September's terrorist attacks to a number of malicious and highly publicized computer viruses — reminded every one of us how important it is to ensure the integrity and security of our critical infrastructure, whether it's the airlines or computer systems.

Computing is already an important part of many people's lives. Within 10 years, it will be an integral and indispensable part of almost everything we do. Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing.

Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched — but as an industry leader we can and must do better. Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these

fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it.

No Trustworthy Computing platform exists today. It is only in the context of the basic redesign we have done around .NET that we can achieve this. The key design decisions we made around .NET include the advances we need to deliver on this vision. Visual Studio .NET is the first multi-language tool that is optimized for the creation of secure code, so it is a key foundation element.

I've spent the past few months working with Craig Mundie's group and others across the company to define what achieving Trustworthy Computing will entail, and to focus our efforts on building trust into every one of our products and services. Key aspects include:

Availability: Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.

Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level — from the way we develop software, to our support efforts, to our operational and business practices. As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable. Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company.

In recent months, we've stepped up programs and services that help us create better software and increase security for our customers. Last fall, we launched the Strategic Technology Protection Program, making software like IIS and Windows .NET Server secure by default, and educating our customers on how to get — and stay — secure. The error-reporting features built into Office XP and Windows XP are giving us a clear view of how to raise the level of reliability. The Office team is focused on training and processes that will anticipate and prevent security problems.

In December, the Visual Studio .NET team conducted a comprehensive review of every aspect of their product for potential security issues. We will be conducting similarly intensive reviews in the Windows division and throughout the company in the coming months.

At the same time, we're in the process of training all our developers in the latest secure coding techniques. We've also published books like Writing Secure Code, by Michael Howard and David LeBlanc, which gives all developers the tools they need to build secure software from the ground up. In addition, we must have even more highly trained sales, service and support people, along with offerings such as security assessments and broad security solutions. I encourage everyone at Microsoft to look at what we've done so far and think about how they can contribute.

But we need to go much further.

In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a

terrific job at that, but all those great features won't matter unless customers trust our software.

So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid e-mail-borne viruses. If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.

What does Gates mean when he says "[s]ystems will have to become self-managing and inherently resilient?"

Going forward, we must develop technologies and policies that help businesses better manage ever larger networks of PCs, servers and other intelligent devices, knowing that their critical business systems are safe from harm. Systems will have to become self-managing and inherently resilient. We need to prepare now for the kind of software that will make this happen, and we must be the kind of company that people can rely on to deliver it.

This priority touches on all the software work we do. By delivering on Trustworthy Computing, customers will get dramatically more value out of our advances than they have in the past. The challenge here is one that Microsoft is uniquely suited to solve.

More discussion of our vision for Trustworthy Computing is in the internal white paper.

Bill

Notes and Questions

What motivates this memo? Is Microsoft's "Trustworthy Computing" the same as Stefik's "trusted systems"? What is Gates suggesting was the state of affairs for Microsoft developers – and the software they write – before this memo came about?

Steven Levy
"The Big Secret"
July 1, 2002 issue of Newsweek
Available at: http://www.msnbc.com/news/770511.asp?cp1=1

Here's something that cries for a safeguard: the world of computer bits. An endless roster of security holes allows cyber-thieves to fill up their buffers with credit-card numbers and corporate secrets. It's easier to vandalize a Web site than to program a remote control. Entertainment moguls boil in their hot tubs as movies and music are swapped, gratis, on the Internet. Consumers fret about the loss of privacy. And computer viruses proliferate and mutate faster than they can be named.

Computer security is enough of a worry that the software colossus Microsoft views it as a threat to its continued success: thus the apocalyptic Bill Gates memo in January calling for a "Trustworthy Computing" jihad. What Gates did not specifically mention was Microsoft's hyperambitious long-range plan to literally change the architecture of PCs in order to address the concerns of security, privacy and intellectual property. The plan, revealed for the first time to NEWSWEEK, is... Palladium, and it's one of the riskiest ventures the company has ever attempted. Though Microsoft does not claim a panacea, the system is designed to dramatically improve our ability to control and protect personal and corporate information. Even more important, Palladium is intended to become a new platform for a host of yet-unimagined services to enable privacy, commerce and entertainment in the coming decades. "This isn't just about solving problems, but expanding new realms of possibilities in the way people live and work with computers," says product manager Mario Juarez.

Because its ultimate success depends on ubiquity, Palladium is either going to be a home run or a mortifying whiff. "We have to ship 100 million of these before it really makes a difference," says Microsoft vice president Will Poole. That's why the company can't do it without heavyweight partners. Chipmakers Intel and Advanced Micro Devices have signed on to produce special security chips that are integral to the system. "It's a groundswell change," says AMD's Geoffrey Strongin. "A whole new class of processors not differentiated by speed, but security." The next step is getting the likes of Dell, HP and IBM to remake their PCs to accommodate the system.

"It's one of the most technically complex things ever attempted on the PC," says Gartner analyst Martin Reynolds. And the new additions will make your next computer a little more expensive. Will the added cost—or a potential earlier-than-otherwise upgrade—be worth it? Spend a day or two with the geeks implementing Palladium—thrilled to be talking to a reporter about the project—and you'll hear an enticing litany of potential uses.

Tells you who you're dealing with—and what they're doing. Palladium is all about deciding what's trustworthy. It not only lets your computer know that you're you , but also can limit what arrives (and runs on) your computer, verifying where it comes from and who created it.

Protects information. The system uses high-level encryption to "seal" data so that snoops and thieves are thwarted. It also can protect the integrity of documents so that they can't be altered without your knowledge.

Stops viruses and worms. Palladium won't run unauthorized programs, so viruses can't trash protected parts of your system.

Cans spam. Eventually, commercial pitches for recycled printer cartridges and barnyard porn can be stopped before they hit your inbox—while unsolicited mail that you might want to see can arrive if it has credentials that meet your standards.

Safeguards privacy. With Palladium, it's possible not only to seal data on your own computer, but also to send it out to "agents" who can distribute just the discreet pieces you want released to the proper people. Microsofties have nicknamed these services "My Man." If you apply for a loan, you'd say to the lender, "Get my details from My Man," which, upon your authorization, would then provide your bank information, etc. Best part: Da Man can't read the information himself, and neither can a hacker who breaks into his system.

Controls your information after you send it. Palladium is being offered to the studios and record labels as a way to distribute music and film with "digital rights management" (DRM). This could allow users to exercise "fair use" (like making personal copies of a CD) and publishers could at least start releasing works that cut a compromise between free and locked-down. But a more interesting possibility is that Palladium could help introduce DRM to business and just plain people. "It's a funny thing," says Bill Gates. "We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains." For instance, Palladium might allow you to send out e-mail so that no one (or only certain people) can copy it or forward it to others. Or you could create Word documents that could be read only in the next week. In all cases, it would be the user, not Microsoft, who sets these policies.

Some of these ideas aren't new—they're part of the promise of public key cryptography, discovered 25 years back. Palladium is a dead-serious attempt to finally make it happen, with a secure basis and critical mass. But it didn't start that way. In 1997, Peter Biddle, a Microsoft manager who used to run a paintball arena, was the company's liason to the DVD-drive world. Naturally, he began to think of ways to address Hollywood's fear of digital copying. He hooked up with ' Softie researchers Paul England and John Manferdelli, and they set up a skunkworks operation, stealing time from their regular jobs to pursue a preposterously ambitious idea—creating virtual vaults in Windows to protect information. They quickly understood that the problems of intellectual property were linked to problems of security and privacy.

They also realized that if they wanted to foil hackers and intruders, at least part of the system had to be embedded in silicon, not software. This made their task incredibly daunting. Not only would they have to build new secrecy functions into Windows (without messing up any programs that run on the current versions), but then they'd have to convince the entire industry to, in effect, update the basic hardware setup of the PC.

Intel originally turned down the idea before eventually embracing it. AMD had already been thinking along similar lines, and eagerly signed on. Biddle's virtual team kept working, and in October 2001, it became a formal green-lighted project.

As now envisioned, Palladium will ship "in a future version of Windows." (Perhaps in the next big revision, due around 2004.) By then the special security chips will be rolling out of the fabs, and the computer makers—salivating at an opportunity to sell more boxes—will have motherboards to accommodate them. There will also be components that encrypt information as it moves from keyboard to computer (to prevent someone from wiretapping or altering what you type) and from computer to screen (to prevent someone from generating a phony output to your monitor that can trick you into OKing something you hadn't intended to). Only certain applications will access the part of Windows (nicknamed "the nub") that performs Palladium's functions with the help of the security chip—everything else will work exactly the same.

The first adopters will probably be in financial services, health care and government—places where security and privacy are mandated. Then will come big corporations, where information-technology managers will find it easier to control and protect their networks. (Some employees may bridle at the system's ability to ineluctably log their e-mail, Web browsing and even instant messages.) "I have a hard time imagining that businesses wouldn't want this," says Windows czar Jim Allchin.

Finally, when tens of millions of the units are in circulation, Microsoft expects a flood of Palladium-savvy applications and services to spring up—that's when consumers will join the game.

None of this is a cinch. One hurdle is getting people to trust Microsoft. To diffuse the inevitable skepticism, the Redmondites have begun educational briefings of industry groups, security experts, government agencies and civil-liberties watchdogs. Early opinion makers are giving them the benefit of the doubt. "I'm willing to take a chance that the benefits are more than the potential downside," says Dave Farber, a renowned Internet guru. "But if they screw up, I'll squeal like a bloody pig." Microsoft is also publishing the system's source code. "We are trying to be transparent in all this," says Allchin.

Others will note that the Windows-only Palladium will, at least in the short run, further bolster the Windows monopoly. In time, says Microsoft, Palladium will spread out. "We don't blink at the thought of putting Palladium on your Palm... on the telephone, on your wristwatch," says software architect Bryan Willman.

And what if some government thinks that Palladium protects information too much? So far, the United States doesn't seem to have a problem, but less tolerant nations might insist on a "back door" that would allow it to wiretap and search people's data. There would be problems in implementing this, um, feature.

Other potential snags: will Microsoft make it easy enough for people to use? Will someone make a well-publicized crack and destroy confidence off the bat? "I firmly believe we will be shipping with bugs," says Paul England. Don't expect wonders until version 2.0. Or 3.0. Ultimately, Palladium's future defies prediction. Boosting privacy, increasing control of one's own information and making computers more secure are obviously a plus. But there could be unintended consequences. What might be lost if billions of pieces of personal information were forever hidden? Would our ability to communicate or engage in free commerce be restrained if we have to prove our identity first? When Microsoft manages to get Palladium in our computers, the effects could indeed be profound. Let's hope that in setting the poli-

cies for its use, we keep in mind the key attribute of the woman embodied in the first Palladium. Athena was the goddess of wisdom.

Jonathan Zittrain

"Taming the Consumer's Computer"

New York Times, March 11, 2002

CAMBRIDGE, Mass.

Last month the top executives of two of the most powerful media companies in the world traveled to Washington to testify before Congress about the most dangerous threat they face: the American consumer.

Of course they didn't quite phrase it that way. Michael Eisner, chief executive of the Walt Disney Company, complained that the technology industry made it too easy for "people wanting to get anything for free on their television or computer or hand-held device." Peter Chernin, president of the News Corporation, worried that the Internet's "ability to empower the general public" would lead to the online theft of some of the contents of media companies' digital treasuries.

Both men want the next generation of personal computers to be unable to deliver unauthorized movies, music and other content, and they asked that Congress stand ready to intervene if industry failed to deliver the necessary technology to safeguard its products. A lone executive, from Intel, objected. The market, he said, not Congress, should dictate how technology works.

The debate on Capitol Hill between content providers like Disney and those who make the products to deliver that content, like Intel, was really a proxy for a much larger debate: What do we want our technology to do? How do we want it to work? And do we have any say in the matter?

For most forms of current technology, these questions have long been settled. No executives are worried about illegal uses of televisions or coffee makers, for instance, and no consumers need to worry that these appliances will crash or become infected with viruses — and we would never accept it if they did. Our TV's and VCR's don't take ill when we watch infected programs, and our refrigerators never require rebooting.

Yet we have come to tolerate such problems from our personal computers. The PC's fundamental and unique unreliability flows from its construction as a so-called flexible platform — a mere staging area for many kinds of software. The point (and bane) of a PC is, essentially, to run whatever software it encounters.

There are plenty of reliable computers: the controls of the modern Airbus 340 are fully given over to a computer, and video-game consoles consistently work as advertised, as do Aegis missile cruisers, cellular telephones and digital watches. All contain transistors. Can technologists figure out how to replicate the reliability of airplanes, telephones, watches and televisions in future versions of Windows and Linux, so that a mischievous 12-year-old half a world away can't erase a thousand far-flung hard drives?

Absolutely. In January Bill Gates sent a memo to all Microsoft employees declaring a new, overarching, even revolutionary mandate: Software must be reliable and "trustworthy." This new focus is both welcome and worrisome, because the very steps needed to secure our computers and networks can be the steps that will deaden them to continued innovation and creative uses — while opening them to more intrusive monitoring by mainstream technology manufacturers and content providers.

Mr. Gates and the co-captains of his industry are producing blueprints for so-called "trusted" PC's. They will employ digital gatekeepers that act like the bouncers outside a nightclub, ensuring that only software that looks or behaves a certain way is allowed in. The result will

be more reliable computing — and more control over the machine by the manufacturer or operating system maker, which essentially gives the bouncer her guest list.

And as soon as there are limits on the software a PC can run, there will be limits on what PC users can do. That's exactly what executives like Mr. Eisner and Mr. Chernin want. They'd like software and hardware companies to build PC's to allow a publisher an exquisite level of control over a book or a song or a movie in the hands of a consumer. Trusted PC users might spend $1.95 for a single viewing of the latest Disney animated feature, or they might pay a similar amount for three listens of U2's most recent single. Security, stability, reliability — and control.

Users may buy a trusted PC even if it won't show a digital video lent by a friend, because it will act less like a temperamental computer and more like a crash-free super-VCR — like the just-released Microsoft X-box. But in the process of "improving" our PC's, the manufacturers and their partners will be able to determine what software will and won't be allowed to run, what we can and can't do with the information to which we're exposed, and what data about our online activities will be collected and sent to the manufacturer or content provider to assist in future marketing.

Apart from manufacturers' desire not to define the uses of a PC too narrowly, the public interest in flexible computer platforms and open data exchange remains almost entirely absent from this debate. Disney and its cohort are free to view PC's as delivery systems for Mickey Mouse and friends — and to make their content available through broadband. But it's an entirely different matter to re-engineer the PC so it becomes simply another appliance.

The PC platform and the Internet to which it connects is the engine of the information revolution — as important to our economy and culture as all the movies in Hollywood. A shift from open platforms to closed appliances may be inevitable, as our consumerist desire for trustworthy PC's dovetails with information providers' obsession with control. But we should beware the haste with which some would sacrifice flexibility for control. If we can't at least temper this taming of the chaotic PC, the victims will be competition, innovation and consumer freedom.

3. Trusted Systems: Examples and Discussion

a. Circuit City's Divx

Launched in 1998 after four years' development, Divx was a proprietary digital video format backed mainly by a chain of electronics stores called Circuit City. (This is not to be confused with DivX, a common means of compressing video for easy Internet transmission.) Playable only on "Divx-enabled DVD players" (in fact, Divx was a distinct video format from DVD and not a feature layered on top of DVD), Divx discs would retail for approximately five dollars. The discs and player comprised a trusted system that would only allow a viewer to watch the disc for a 48-hour period and only on his or her player. In this way, Circuit City hoped to offer the convenience of video rental without the bite of exorbitant late fees and the hassle of returning videos to stores once watched.

Chris Stamper
"Is Video Rental a Goner?"
ABCNEWS.com, March 28, 1998
Available at: http://more.abcnews.go.com/sections/tech/DailyNews/dvd_divx.html:

Even though a mere one-tenth of 1 percent of American homes now use DVD, a pay-per-view variation will launch this year called Divx, or Digital Video Express. Instead of renting a tape, video stores sell a special $4.49 DVD disc with a Mission Impossible twist. Two

days after you pop the platter in your player, it shuts down and becomes digitally encrypted garble.

Divx promises the convenience of a trip to the video store without the inconvenience of returning the tape. The system includes not only a specially formatted DVD, but also a proprietary player that includes a jack to attach a player to the standard phone line for billing purposes.

Spokesman Josh Dare says Divx discs are for home users who want to rent Titanic or Men In Black, not videophiles who want 28 versions of Army of Darkness. "Divx is not for everybody," he acknowledges. "It's for the family video renter who wants to avoid the late fee."

The Richmond, Va.-based Circuit City electronics chain, majority owner of Divx Inc., will test its system this spring and plans a nationwide release this summer. Five hundred titles are promised in Divx's first year, from Disney, Paramount, Fox, Universal and DreamWorks. Licensed movies will be released on the same day as their VHS counterparts. Also, Divx says it will not allow adult-movie makers to use its format.

Credit-Card Connection

For billing, users set up an account with Divx and attach their player to a standard phone line. The machine calls up the home office in North Carolina and updates charges to the customer's credit card. (Divx promises not to provide account information to third parties.)

Pay another 12 bucks and your dead platter can become a DivxSilver disc that can be used indefinitely. The catch is that only players using the owner's account can play the disc; friends and neighbors must pay another rental charge. Also, the signal is encoded with Macrovision, a popular copy-protection system, to discourage copying onto a VHS tape or recordable DVD.

To keep hackers from bypassing the payment system, Divx brings strong encryption off the Web and into home video. It uses a 112-bit, double-key system similar to the security systems developed by the military and now used by electronic commerce sites. "This is the same technology the U.S. sold Saddam Hussein back when we were friends with Iraq," Dare says.

By all accounts, Divx was a major failure for Circuit City. Some claim consumers simply favored the standard DVD format and the greater degree of control it affords. Others point to the incompatibility between the Divx disc and non-Divx-enabled players; only a handful of Divx-enabled models were available, mainly at Circuit City stores. Lastly, Circuit City failed to get the critical support it needed from the movie studios. Very few titles were made available in the Divx format relative to the wide availability of DVD movies. All of these factors likely operated in an interrelated manner; Divx simply failed to achieve "critical mass." In June of 1999, Circuit City pulled the plug on the venture, having lost over $100 million.

What reason is there to think that any one company's attempt to define new standards for content control within new products – incompatible with those of others – will succeed? Is Microsoft any more strategically positioned than Circuit City to make it happen?

b. Nondigital trusted systems

In most cities, the fares charged to passengers in taxi cabs are computed and stored by a trusted system. Colloquially termed "the meter," this trusted system guarantees the accuracy of the mileage and timing figures used to compute the fare and provides locks to ensure that the system is not tampered with. There are many examples of "real world" trusted systems such as this one that function to introduce trust into commercial transactions. (For example, gas pumps at gas stations employ a similar system to monitor the volume of gas pumped.)

In most cities, the use of taxi cab meters is highly regulated. In Section <X>, we discuss thoroughly the use of public law to mandate compliance with technologies that protect copyright interests. As is the case with taxi

cab meters, the law mandates compliance with protective technologies in many other industries, serving a variety of functions.

c. Electronic books

The eBook Reader is a trusted system that, together with a proprietary, encrypted file format for representing books digitally, protects the copyright interests of authors (or their publishers) wishing to make books available in digital form. In Section <X>, we discuss the criminal prosecution of Dmitry Sklyarov and Elcomsoft under the Digital Millennium Copyright Act for circumventing the technology controls embedded in Adobe Acrobat's eBook Reader.

4. From firms to industries: E pluribus unum

So far we have reviewed examples of individual firms attempting to devise trusted systems. The "critical mass" problem is significant, enough so that intra-industry working groups have come about to attempt to unify corporate efforts on trusted systems. Just as various firms might come together to determine a common configuration for electrical outlets and the plugs to be inserted into them, the computing industry as a whole has, in fitful steps, taken on the project of devising common standards for security generally and trusted systems specifically. Such a project always has within it the prospect that a larger player might peel off and attempt to build a proprietary system to capture the whole market – not unlike the battle between Sony and a consortium led by RCA over VCR tape standards, Beta vs. VHS.

Mark A. Lemley
Intellectual Property Rights and SSOs – DRAFT
Available at: http://www.ftc.gov/opp/intellect/020418lemley.pdf

> Standard-setting organizations (SSOs) are industry groups that set common standards in a variety of significant areas. Telephones talk to each other, the Internet works, and hair dryers plug into electrical sockets because private groups have set "interface" standards allowing products made by different manufacturers to be compatible. In such interface standards, it is important that different companies be able to make products that comply with the standard.
> …
>
> A. The Value of Standardization
>
> Standards (and standard-setting organizations) come in a variety of forms. … Some standards are extremely complex and technical in nature. For example, the set of applications programming interfaces that defines compatibility with the Microsoft Windows operating system is an industry standard; those who know and use the proper interfaces are compliant with the standard, and their products will "interoperate" with the Microsoft OS. But standards do not have to be so sophisticated. Ordinary consumers use a wide variety of standardized products in everyday life. In the U.S., electrical plugs and outlets are built to a particular standard for voltage, impedance, and plug shape. Without this standardization, no one could stay in a hotel room and have any confidence that their hair dryer would work in the hotel's outlet. The modern economy has also standardized telephone service, computer modem communication protocols, automobile ignition and transmission systems, and countless other products.
>
> As these examples attest, in many markets standardization has significant consumer benefits. This is especially true in so-called "network markets," where the value of a product to a particular consumer is a function of how many other consumers use the same (or a compatible) product. The paradigm example is the telephone network, in which the value of the product is entirely driven by the number of other people on the same network. Still other

products — like computer operating systems — have some intrinsic value regardless of how many people use them, but gain value as more and more consumers adopt them. In these industries, consumers benefit from standardization not only because they can reliably use their product in a remote location, but also because they can exchange information with others who use the same standard. Further, markets for complementary products will often gear their production to work with a product that is an industry standard, rather than a product that has only a small market share. For example, software vendors are more likely to write computer applications programs compatible with Microsoft's operating system than with other operating systems, because there are more consumers for such a product. This in turn reinforces the desire of consumers to buy the product everyone else buys, a phenomenon known as "tipping."

In network markets, then, standardization may well be inevitable, and certainly carries substantial consumer benefits. Even in non-network markets, standard-setting can have a variety of procompetitive and other beneficial effects. Agreeing on a set of standards can facilitate a competitive market for replacement parts or service in durable goods industries, for example. Further, in many industries standards may be valuable for reasons unrelated to or even inimical to competition. Construction products must meet industry standards for fire resistance, for example, and doctors, lawyers and many other professionals must meet minimum licensing standards. These latter standards are not procompetitive in the narrow sense of encouraging price competition; indeed, they may have the opposite effect. But standards of this type can still promote social welfare by ensuring that imperfect information does not lead consumers to buy dangerous products or hire unqualified doctors simply because they cost less.

While standardization can be beneficial in a wide variety of markets, it is worth distinguishing at the outset between two different types of standards - standards that control interoperability in a network market and those that govern the quality or safety of a product. In the former group, which I will call "network" or "interface" standards, the intrinsic value of the standard selected is only part of the social benefit of standard-setting. Simply agreeing on a standard for two products to interact has value in a network market, whether the interface actually chosen is the best one or not. Indeed, in some cases it may be more important that an industry coalesce around a single standard than which particular standard is chosen. By contrast, standard-setting outside network markets tends to be concerned primarily with the intrinsic value of the product itself. These latter standards may guarantee minimum licensing qualifications for the professions, or specify safety codes that consumer products must meet.

Is Palladium a "network standard" or simply a "product standard"? How about a taxicab meter?

…

B. The Benefits of Group Standard-Setting

It remains, however, to consider the organizational form standardization may take. One approach to achieving interoperable standards is for a private industry organization open to all members to adopt a single standard. If the members of such a group collectively have a significant market share, their adoption of a standard may produce the "tipping" effect described above, bringing the rest of the industry into line.

Not all standards are created by private standard-setting organizations, however. Two other organizational forms are worth considering. First, a standard may arise from the operation of the market, as consumers gravitate towards a single product or protocol and reject its competitors. This form of "de facto" standardization is particularly likely in markets characterized by strong network effects, because of the large benefits associated with adopting the same product everyone else does. To take just one example, the Microsoft operating systems are clearly de facto standards. No standard-setting organization "adopted" them as the preferred or official operating systems, but the market clearly chose Microsoft as the winner of a standards competition.

For more on the IETF, see chapter <X>.

Another possibility is that the government might identify and set the appropriate standards and compel all participants in the market to comply. The government does this from time to time. For example, the Federal Communications Commission sets standards for interconnection between telephone networks and standards governing the use of products that might interfere with broadcast communications. In the 1990s, the United States government stepped into the debate over the proper standard for high definition television (HDTV), selecting a standard that unified U.S. development work but was at odds with other standards adopted in Japan and Europe. And government agencies such as the Advanced Research Projects Agency and the National Science Foundation played a crucial role in the development of the Internet, including the creation of Internet interconnection protocols. Indeed, some private Internet standard-setting groups such as InterNIC and the IETF were once government-sponsored standards organizations.

5. The Secure Digital Music Initiative

One of the most widely publicized efforts to replace crumbling intellectual property shields with newer, stronger technological shields has been the Secure Digital Music Initiative (SDMI).

Q&A on SDMI
Interview with Talal Shamoon, SDMI technologist
Salon.com, July 31, 2000

SDMI is a standards body which is sort of intent on finding ways for open MP3s to cohabit with protected music. What SDMI serves to do is create a parameter between the open world and this new protected world at least in order to buy the protected world a little bit of space while people fill it with music.

Q. How do the members of SDMI plan to do this?

A. The specification that's been written so far speaks to two things. One is a set of good housekeeping tips on how to keep protected music protected. So it's not a specific technology. All the specification says is, "if you download a song to a PC it should be protected; if you transfer it to a portable device, the wire along which it travels should be protected and the portable device itself should keep it protected." How you do that is up to you as long as you conform to these rules.

The other part of SDMI is more specific. It talks about screening technology, which at this point uses a specific set of algorithms from a company called Verance. The goal of the screening technology is to solve the following problem: You have an SDMI portable device that plays protected music. You want to let people transfer MP3s they've ripped to that portable device. You don't want to let them transfer MP3s they've gotten from somebody else who's ripped them, i.e. from something like Napster. And what you want is technology that basically examines an open MP3 file that's being transferred to a portable device and decides whether or not it should be admitted to the portable device.

So in order to do that, there's a call for technology from different parties to provide that screening system. We're about a third of the way there. Today, in deployment, we have an algorithm by Verance that's sitting there dormant waiting to be activated.

Q. How does it work?

A. It's watermarking, which uses a set of techniques to hide a message in a signal. Usually what you do is place a message in part of a signal that makes it inaudible but very hard to remove. There's an assortment of tricks for doing that. That's the essence of watermarking.

And the message can say anything you want it to. Usually they're short messages that say one of two things. The SDMI phase one message says either we're in phase one or phase two has started. If it says phase two has started, then a trigger piece of software tells the user that they need an upgrade. This upgrade implements the phase two screening technology, which looks for misappropriated content and then blocks it from being transferred, or just decides the content isn't misappropriated and lets it through.

Phase two technology hasn't been chosen yet. So all we have in place is the technology for the trigger. And music companies — all of the majors have made noise about it — are saying that they'll be shipping content with trigger capacity in it over the next month or two.

Q. But this watermarking won't do anything for the millions of songs that are already available online as MP3s ...

A. Nope.

Q. Are there any plans to try and put these under the SDMI umbrella?

A. No. I would be amazed to see technology that could do that. That's sort of like calling the missiles back.

In September of 2000, after a development process that lasted much longer than expected, SDMI made available to the public prototypes of its new watermarking system – a type of trusted system – and invited hackers to try to break it. To the consternation of the developers, the systems were broken promptly by Professor Edward Felten. <X>Reference to Felten DMCA controversy, wherever it winds up (in text, supplement, web, etc.).

The SDMI's website features a report on its "current status" dated May 18, 2001, which states: "Based on all of the factors considered by the SDMI plenary, it was determined that there is not yet consensus for adoption of any combination of the proposed technologies. Accordingly, SDMI is now on hiatus, and intends to re-assess technological advances at some later date." On April 29, 2002, the Associated Press reported: "… SDMI is roadkill, outpaced by developments in digital technology and done in by the narrow interests of its own members – record labels competing for dominance and music hardware companies impatient to get their products out to consumers", not to mention the debacle over Professor Felten's hack.

Notes and Questions

1) Edward Felten: cracking SDMI

The Secure Digital Music Initiative (SDMI) – an effort to develop trusted system technology to guarantee copyrights in digital music – was discussed earlier in this chapter. On September 6, 2000, the SDMI issued "An Open Letter to the Digital Community," stating in part:

> We are now in the process of testing the technologies that will allow these protections. The proposed technologies must pass several stringent tests: they must be inaudible, robust, and run efficiently on various platforms, including PCs. They should also be tested by *you*.
>
> So here's the invitation: Attack the proposed technologies. Crack them.
>
> By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt. And there is something more in it for you, too. If you can remove the watermark or defeat the other technology on our proposed copyright protection system, you may earn up to $10,000.

(A copy of this invitation is posted at http://www.sdmi.org/pr/OL_Sept_6_2000.htm.)

Edward Felten, a computer scientist at Princeton, successfully "broke" the code for the SDMI watermark prototypes. When Felten made public his intention to publish an article describing how he was able to do so, the RIAA sent him a letter suggesting that such publication "could subject [him] and [his] research team to actions under the DMCA." In response, Felten brought a declaratory judgment action against the RIAA, the SDMI Project, and the United States in federal court in New Jersey, seeking a ruling either that the statutory prohibition on "trafficking" in circumvention technology did not apply to his proposed publication or that, if it did apply, it would be unconstitutional.

The defendants backed down, insisting that they never intended to bring suit. Judge Garrett Brown, writing for the Federal District Court in Trenton, New Jersey, dismissed the case November 28, 2001. Professor Felten decided not to appeal this decision.

Did Edward Felten violate the DMCA by trafficking in circumvention technology? Does your answer depend on whether he published an executable program or just a paper describing his algorithms? Could he have invoked any exceptions?

2) Sony's "copy-proof cds":

> Consider the failure of Sony's latest technological initiative to protect its digital music, the "copy-proof CD." As Reuters reported on May 20, 2002:
>
> Technology buffs have cracked music publishing giant Sony Music's elaborate disc copy-protection technology with a decidedly low-tech method: scribbling around the rim of a disk with a felt-tip marker."
>
> …
>
> The new technology aims to prevent consumers from copying, or "burning," music onto recordable CDs or onto their computer hard drives, which can then be shared with other users over file-sharing Internet services such as Kazaa or Morpheus MusicCity.
>
> On Monday, Reuters obtained an ordinary copy of Celine Dion's newest release "A New Day Has Come," which comes embedded with Sony's "Key2Audio" technology.
>
> After an initial attempt to play the disc on a PC resulted in failure, the edge of the shiny side of the disc was blackened out with a felt tip marker. The second attempt with the marked-up CD played and copied to the hard drive without a hitch.

The full article is available at http://www.wired.com/news/technology/0,1282,52665,00.html.

Has Reuters violated the DMCA? What claims could be brought against Reuters under the statute? Which are most promising? Under what conditions, if any, could a seller of markers be charged with trafficking in "circumvention technology?"

3) Consider the potential damage or disruption that copy-proof compact discs can cause a computer system. As reported by John Leyden in his May 14, 2002 article for theregister.co.uk, "Marker pens, sticky tape crack music CD protection":

> Epic/Sony's release of Celine Dion's A New Day Has Come audio disc this month, which included copy protection technology from Key2Audio, caused a furore after online sites reported that attempts to play the disc on a PC caused computers to crash.
>
> The problem can be even more severe for Mac users.
>
> Not only will the Celine Dion audio disc fail to play on new flat-screen iMacs but it will lock the CD tray and prevent the machine from been rebooted properly. This is not something users can fix themselves and means a trip to a dealer for repairs.

(The story is available at: http://www.theregister.co.uk/content/54/25274.html)

Does this effect your analysis? Does a user violate the DMCA if he or she circumvents Sony's Key2Audio system for the sole purpose of listening to – not "ripping" – a disc he or she has purchased?

4) The introduction of copy-proof cds – and the ease of circumventing them – highlights the potentially vast reach of the DMCA. Naturally, they also serve to illustrate the challenge industries face in developing meaningful technological controls and the monumental failures that often result. Does the DMCA bolster even utterly ineffective technologies? Does Sony's Key2Audio technology "effectively control[] access to a work protected under [copyright]"? 17 U.S.C. 1201(a)(1)(A).

6. The Trusted Computing Platform Alliance

The Trusted Computing Platform Alliance ("TCPA") is an organization founded in October of 1999 by leaders of the hardware manufacturing and software development industries. The TCPA's website, located at <http://www.trustedpc.org>, discloses its mission: "Through the collaboration of [hardware, software,] communications, and technology vendors, drive and implement TCPA specifications for an enhanced [hardware] and [operating system] based trusted computing platform that implements trust into client, server, networking, and communication platforms."

Are the TCPA standards "network standards"?

In January of 2001, the TCPA released the first version of its Specification for Trusted Computing. This specification calls for the incorporation of specialized "security" chips into personal computers. These chips – dubbed Trusted Platform Modules, or TPMs – perform a variety of functions to enhance system security, including: generating and storing digital certificates and private keys, supporting multiple authentication schemes and encrypting / decrypting files on demand.

In April of 2002, IBM, one of the founding members of the TCPA, released the first compliant hardware system. Some models of its ThinkPad T30 high-end notebook include a TCPA TPM.

With over 180 members, the TCPA is currently working on version 1.2 of its Specification for Trusted Computing. For more information on the TCPA, visit its website at <http://www.trustedpc.com>.

Notes and Questions

How can 180 members come to agreement on anything? How important would representation in such a group be to a company that produces digital music players? How important would it likely be to Microsoft? To IBM? What is likely to happen if a company decides to ignore an agreed-upon standard?

7. Social Implications of Trusted Systems

1) Do you think trusted systems ultimately benefit consumers by providing content producers the protections they require before making content available in digital formats? That is, absent trusted systems to protect digital content, would producers simply refuse to make such content available? Do content producers have to make their content available in new, digital formats to stay competitive, notwithstanding a lack of protective technologies?

2) How likely is it that consumers will embrace trusted systems as platforms that deliver new features and a wider array of pricing options? Will consumers "finally" be able to pay only for the uses they desire, or is it unlikely that they'll be able to obtain – or retain – the uses they really want? Will content producers employing trusted systems gain an unprecedented level of control over their content – an unprecedented ability to exploit their rights in such content and track users' interactions with it?

Mark Stefik

Trusted Systems

Scientific American, March 1997.

What's in all this for consumers? Why should they welcome an arrangement in which they have less than absolute control over the equipment and data in their possession? Why should

they pay when they could get things for free? Because unless the intellectual-property rights of publishers are respected and enforced, many desirable items may never be made digitally available, free or at any price. Trusted systems address the lack of control in the digital free-for-all of the Internet. They make it possible not only for entire libraries to go on-line but also for bookstores, newsstands, movie theaters, record stores and other businesses that deal in wholly digital information to make their products available. They give incentives for 24-hour access to quality fiction, video and musical works, with immediate delivery anywhere in the world. In some cases, this technological approach to protecting authors and publishers may even avoid the need for heavy-handed regulations that could stifle digital publishing.

Fully realizing this vision will necessitate developments in both technology and the marketplace. Users will need routine access to more communications capacity. Publishers must institute measures to ensure the privacy of consumers who use trusted systems, although the same technology that guards the property rights of publishers could also protect personal details about consumers. Trusted systems also presume that direct sales, not advertising, will pay the costs of distributing digital works. Advertising will most likely prevail only for works with substantial mass-market appeal. By protecting authors' rights, trusted systems will enable specialized publishing to flourish: compare, for instance, the diverse collection of books in a library to the relative paucity of programs for television.

The dynamics of a competitive marketplace form the most imposing roadblock to fashioning protections for digital rights. Several companies have trusted systems and software in the early stages of testing. With some exceptions, though, the software is proprietary and incompatible. Whereas the technology could provide the infrastructure for digital commerce, the greatest benefits will accrue only if the various stakeholders, from buyers and sellers to librarians and lawmakers, work together.

Harvey Weinberg

Hardware-Based ID, Rights Management, and Trusted Systems

52 Stan. L. Rev. 1251

Widespread deployment of trusted systems based on such global identifiers will have social consequences. Such systems - in which the user's computer identifies itself during every transaction, to anybody who asks - are pernicious from a privacy perspective. They allow the user to be tracked through cyberspace more easily and thoroughly than is possible under current technology. They have the potential to make the Internet a forum in which database proprietors have what Phil Agre has referred to as a "God's-eye view of the world" - a perspective in which all things have their true names and our Internet representations can straightforwardly be traced back to our real-world identities. Under such an architecture, a much greater proportion of ordinary transactions would require consumers to present unique identification numbers that would in turn be digitally linked to a much wider range of personal information. To the extent that collecting identification and assembling dossiers is easy, content providers may do so even when they have no compelling use for the information.

Advertisers and others already see great value in compiling dossiers of personally identifiable information for each of us. Consider, in this regard, the recent Abacus-Doubleclick merger. The combined company announced plans to cross-reference Abacus's database of consumer buying habits, containing real names and addresses and detailed buying information, with Doubleclick's database of consumer Internet surfing and buying habits. Doubleclick targets ads to users, based on "dozens of characteristics, including geographical region, language, and business." It backed off plans to associate its online information about individual consumers with Abacus's personally identifiable offline information only in the face of Federal Trade Commission and state investigations, private lawsuits, and a consumer

boycott. The adoption of common identifiers would facilitate the correlation of individual data profiles across databases without public relations headaches.

Systems facilitating the close tracking of content - of what people read, view, or listen to - seem particularly problematic. All of these are the constituents of human thought. In the analog world, information or entertainment goods are commonly sold on a cash basis, leaving no paper or electronic trail. The copies themselves have no surveillance capabilities, and cannot report back to their makers. The copyright owner, indeed, collects no information about the user at all. Trusted systems threaten to abandon those rules, facilitating the monitoring of individual thought. They raise the specter of the Panopticon, and of subtle and not-so-subtle pressures on individuals to eschew socially or governmentally disfavored information goods.

… [A]ll technological measures protecting digital content (of which trusted systems are a subset) raise an important set of issues typically associated with intellectual property law. Such measures allow sellers of entertainment or information to assert effective control over uses that are privileged by intellectual property law, and over subject-matter that is assigned by intellectual property law to the public domain. That is, they enable sellers to exercise control notwithstanding intellectual property law's judgment that society in those circumstances is best served by free use of the material by the public at large.

Lawrence Lessig

Code and Other Laws of Cyberspace

Basic Books, 1999

... We are not entering a time when copyright is more threatened than it is in real space. We are instead entering a time when copyright is more effectively protected than at any time since Gutenberg. The power to regulate access to and use of copyrighted material is about to be perfected. Whatever the mavens of the mid-1990s may have thought, cyberspace is about to give holders of copyrighted property the biggest gift of protection they have ever known.

In such an age - in a time when the protections are being perfected - the real question for law is not, how can law aid in that protection? but rather, is the protection too great? The mavens were right when they predicted that cyberspace will teach us that everything we thought about copyright was wrong. But the lesson in the future will be that copyright is protected far too well. The problem will center not on copy-right but on copy-duty - the duty of owners of protected property to make that property accessible.

That's a big claim. To see it, however, and to see the consequences it entails, we need consider only two small examples. The first is a vision of a researcher from Xerox PARC (appropriately enough), Mark Stefik, and his idea of "trusted systems."

The second is an implication of a world dominated by trusted systems. Both examples will throw into relief the threat that these changes present for values that our tradition considers fundamental. Both should force us to make a choice about those values, and about their place in our future.

Julie Cohen

The Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace

28 Conn. L. Rev. 981

In truth, … the new information age is turning out to be as much an age of information about readers as an age of information for readers. The same technologies that have made vast amounts of information accessible in digital form are enabling information providers to amass an unprecedented wealth of data about who their customers are and what they like to

read. In the new age of digitally transmitted information, the simple, formerly anonymous acts of reading, listening, and viewing — scanning an advertisement or a short news item, browsing through an online novel or a collection of video clips — can be made to speak volumes, including, quite possibly, information that the reader would prefer not to share.

David G. Post

What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace

(A Review of "Code and Other Laws of Cyberspace" by Lawrence Lessig, Basic Books, 1999)

52 Stan. L. Rev. 1439

(Available at: http://eon.law.harvard.edu/ilaw/Contract/Post_Full.html)

Fundamental values are indeed at stake in the construction of cyberspace, but those values can best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and among different embodiments of those values. We don't need "a plan" but a multitude of plans from among which individuals can choose, and "the market," and not action by the global collective, is most likely to bring that plenitude to us.

...

I have no quarrel with the notion that the code/architectures of cyberspace embed fundamental values, and I have no quarrel with the notion that each of us, confronting the design of these new cyberplaces, faces a choice among different values. It does indeed matter, as Lessig says, whether the code of a cyber-place permits us to be anonymous or not, tracks our mouse droppings or not, allocates to us one screen name or ten, allows us to gather in groups of 20 or 50 or 500, or exposes us to many or to no random encounters.

But I do quarrel with the notion that the choices to be made among value-laden architectures are therefore "political" decisions that should necessarily be subject to "collective" decisionmaking. Consider, by way of counterexample, the original, and still probably the most powerful, value-laden code/architecture of them all: the English language. The semantic and syntactic structures of English (and of all natural languages) are deep architectural constraints on our social life, as the crits … have been fond of pointing out …. Language is not just "a way of communicating propositions about the world," it is "a constitutive social activity," a means by and within which we "construct social reality." Like the network protocols they so closely resemble, these semantic and syntactic structures embed important and often fundamental values throughout.

Each of us, therefore, has choices to make, choices about how our own personal architectures of social reality will be constituted. Notwithstanding powerful "network externalities" in any linguistic system, in which we each gain communicative power when we adopt more "interoperable" rules, the world persists in presenting us with an imposing array of diverse and distinctive linguistic variants. Linguistic communities, subcommunities, sub-subcommunities, and so on, each with its own shared architecture, form and dissolve around us all the time. We can (and should) argue about the ways in which particular linguistic architectures constrain our social worlds; we can (and should) subject the meanings of these code/architectures to discussion, debate, and deliberation; we can (and should) think carefully about the choices each of us has to make about which communities we want to join and which we want to avoid.

But now I get to assert the obvious. I take it as obvious that we do not, and that we should not, subject those semantic and syntactic structures to the collective for decision-making. English will evolve best not by subjecting it to a series of decisions by the collective empowered to impose its will on all, but by an aggregated series of individual and sub-group decisions. We do not have, and we do not want, the Ministry of Semantic Propriety, or our elected representatives, or a specially constituted board of experts, or even the law professors, to

make a "plan" about the proper direction(s) that English may take or to make decisions for us in accordance with that plan. We do not, in fact, have or need a "plan" at all. We are, and should be, deeply suspicious of those who claim to have such a plan, and positively terrified of those who assert that they need to enlist the coercive powers of the State to implement that plan. If there is a serious alternative to the invisible hand that is suitable for this task, I am not aware of it.

...

For it is true: I am as dubious about the need for more politics to help devise the plan for the codes of cyberspace as I am dubious about the need for more politics to help devise the plan for the codes of English. This is not to advocate "doing nothing"; it is to defend the idea that decisions about the contours of the language we speak are best made by individuals and not by collectives. This is not to view English as "the product of something alien - something we cannot direct because we cannot direct anything[, s]omething ... that we must simply accept, as it invades and transforms our lives"; rather, it is to express the belief that the shape of the English language will best emerge not through politics and political processes, but as the aggregate outcome of uncoerced individual decisions. This is not "knee-jerk antigovernment rhetoric," the "pathology of modern politics" that is "so disgusted with self-government that [its] automatic response to government is criticism." If there is a "pathological" position here it is, I suggest, the contrary one, for the history of "collective control" over the use and deployment of natural languages is an ugly one; ask the Armenians, or the Basques, or the Irish, or the Navajo.

Are trusted systems political? More or less political than a language? More or less mandatable than a language?

Notes and Questions

David Post argues that the danger of trusted systems, or control technologies more generally, lies only when governments or commercial bodies of highly centralized control impose them on the masses. He maintains that the architecture of the Internet should be settled by a market of individual actors, not by some collective for decision-making (as Lessig advocates). Thus, in a sense, he combines Stefik's enthusiasm for the promise of trusted systems as developed by the market with Lessig's concern for civil liberties – at least vis-à-vis governments, should they seek to mandate trusted systems.

Is Post necessarily right? Don't you often need the help of government - or a standards-setting coalition comprised of companies that dominate an industry - in order to advance technology? Recall Lemley's enumeration of the benefits of standards-setting, supra page <X>.

Using Legislation to Bolster Technological Controls: The DMCA

Whatever the merits of adopting a set of technologies allowing publishers to restrict and tailor the possible uses of information they've made available, the previous section details some of the difficulties of bringing such a regime about – especially against an extant backdrop of personal computing and network technologies that have no sense of "trustworthiness." While some, like Post, are content to let market forces sort out the success or failure of trusted systems, others have forcefully pressed for a role by governments in encouraging the development or at least dampening the subversion of such systems.

Such encouragement might take as minimal an approach as government purchasing decisions – just as some believe in promoting so-called "open code" by having governments favor such code in the computer systems they purchase and run (see chapter <X>), one could imagine the government certifying only certain kinds of trusted computer systems for its own procurement. More intrusively, the government might simply attempt to mandate trusted systems – as we will see, there are some less ambitious historical antecedents that could suggest such a move.

So far, though, the arguments over government involvement in trusted systems have ranged around "anti-circumvention," by which the development of trusted systems is left to the private sector – while attempts to evade such systems' restrictions are, with some exceptions, given legal penalty by governments. This section begins by exploring in detail the laws covering anti-circumvention, as expressed both in international treaty and within the U.S. legal system, with particular attention to the relevant provisions of the 1998 federal Digital Millennium Copyright Act.

A. The DMCA: Anti-Circumvention Provisions

The Digital Millennium Copyright Act ("DMCA") of 1998 has established both civil and criminal penalties for circumventing technological controls, and distributing technologies developed or marketed to circumvent those controls.

Jonathan Zittrain

What the Publisher Can Teach the Patient: Property and Privacy in an Era of Trusted Privication

52 Stanford L. Rev. 1201 (2000)

> ... [T]he government has been asked by publishers to buttress the security of an imperfect privately deployed trusted system by penalizing those who crack it. The Digital Millennium Copyright Act does just this, providing for civil and criminal penalties for those who circumvent technological protection measures, and in some cases for those who simply make available technologies that can be used for circumvention (and little else). Passage of the DMCA was a high priority for the entertainment industry, and by all accounts its power in the development of the legislation was as strong as with other copyright-related matters taken up by Congress - and the power of disparate "fair use" interests correspondingly weak.
>
> The DMCA's proscriptions are worded in a way that may protect only those trusted systems that contain copyrighted works in the first instance: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." Works protected under Title 17 are works protected by copyright. But this limitation could become a lively area of interpretation. If a trusted system is deployed to protect both copyrighted and non-copyrightable material-whether in the same physical database or not-would cracking the database to gain access solely to the noncopyrightable material be punishable under the DMCA? If so, it is possible that trusted systems covering large databases of unprotectable information could be brought under the DMCA's protection by the mere presence of a copyrighted work elsewhere in the database. However this issue is resolved-and I do not mean to suggest that it will be particularly more vexing than the statutory interpretation issues that courts face every day-it shows that government can choose to enhance the effectiveness of private information control regimes, even aside from legislating substantive information property rights or enforcing contracts.

Larry Lessig

Open Code and Open Society: Values of Internet Governance

Sibley Lecture, University of Georgia, February, 1999

> Now I've made something of a career telling the world that code is law. The rules built into software and hardware functions as a kind of law. That we should understand code as kind of law, because code can restrict or enable freedoms in just the way law should... But in the anti-circumvention of the DMCA, Congress has turned my metaphor into reality. For what the anti-circumvention provision says is that building software tools to circumvent code

that is designed to protect content is a felony. If you build code to crack code then you have violated the US code... Code is law.

Please refer to <X> of <X> for the text of 17 U.S.C. 1201.

Jane C. Ginsburg

Copyright Legislation for the "Digital Millenium"

23 Colum.-VLA J.L. & Arts 137

1. Circumvention of Copyright Protection Systems

…

New section 1201 of the [Digital Millennium Copyright Act] defines three new violations: (a)(1) to circumvent technological protection measures that control access to copyrighted works; (a)(2) to manufacture, disseminate or offer, etc. devices or services, etc. that circumvent access controls; and (b) to manufacture, disseminate, or offer, etc. devices or services etc. that circumvent a technological measure that "effectively protects a right of the copyright owner ...." It is important to appreciate that these violations are distinct from copyright infringement. The violation occurs with the prohibited acts; it is not necessary to prove that the dissemination of circumvention devices resulted in specific infringements.

a. §1201(a): Protection of technological measures controlling access to copyrighted works

This subsection sets out a right to prevent circumvention of technology used to control access to a copyrighted work; the right is articulated separately and treated differently from the circumvention of technology used to protect a "right of the copyright owner" under Title 17 (for instance, to authorize or prohibit reproduction, creation of derivative works, distribution, public performance/display - subsection (b) covers these rights, see infra). The separation of access from rights of copyright owners responds to the different balances struck depending on whether (a) access to the copyrighted work is offered to the public subject to the copyright owner's price and/or terms, or (b) access having been lawfully obtained, members of the public now seek to reproduce/adapt/distribute/publicly perform or publicly display the work (or portions of it).

The DMCA gives the greatest protection to copyright owners' right to control access, since it makes it a violation both (1) for users to circumvent access controls, and (2) for others to manufacture, disseminate or offer devices or services that circumvent access controls. As for post-access circumvention, while the law prohibits the manufacture, dissemination, offering etc. of devices or services, etc. that circumvent technological protection of rights under copyright (e.g., anticopying codes), the bill does not prohibit users themselves from circumventing these protections.

The contrast indicates that this law tolerates direct end-user circumvention of post-access anticopying measures, to a far greater extent than it does circumvention of access controls.

…

b. §1201(a)(1): Prohibition on end-user circumvention of access controls

The DMCA distinguishes between access to the work, and use of the work once accessed. In old technology (hardcopy) terms, the distinction might be between acquiring a copy in the first place, and what one does with the copy thereafter. The fair use concerns primarily focus on the second stage. That is, it may be fair use to make nonprofit research photocopies of pages from a lawfully acquired book; it is not fair use to steal the book in order to make the

photocopies. To that extent, the notion of "access" appears to resemble the traditional copyright concepts inherent in the exclusive distribution right. The Supreme Court has construed this right to give the author

control over the determination to grant "access" to her work, that is, to disclose and offer it to the public, for purchase if she chooses.

i. What is "access"?

…

In adopting an "access to the work" standard, Congress has placed the user who has lawfully stored a copy of an access-controlled work in the same position as a user who does not retain the copy, and who must therefore re-connect to the online source to view the work. Each viewing from the online source is a new "access" to the work. But so are viewings from a downloaded version (or, for that matter, a free-standing version such as a CD ROM). In each of these circumstances, the user may not … circumvent a technological measure that controls the user's ability to apprehend the work.

…

c. §1201(a)(2): Prohibition on manufacture, etc. of devices, etc. that circumvent access controls

If users may not directly defeat access controls, it follows that third parties should not enable users to gain unauthorized access to copyrighted works by providing devices or services (etc.) that are designed to circumvent access controls. Indeed, the principal targets of the DMCA are the providers of circumvention devices, services, etc. As a general proposition, the prohibition on providing devices such as "black box" descramblers that enable members of the public to receive without paying for pay-per-view type transmissions (for example, of music or of audiovisual works), is (or should be) uncontroversial. The question is whether the DMCA's prohibition sweeps too broadly, and ends up barring the manufacture and dissemination of devices or services that have legitimate uses other than to circumvent controls on access to copyrighted works. Too broad a prohibition may frustrate whatever legitimate activities the devices may permit. Equally importantly, too broad a prohibition may frustrate the development of useful new technologies.

Section 1201(a)(2) does not prohibit the dissemination of any device (etc.) that might be used to defeat an access control. It does not target general purpose devices (etc.) whose accidental, incidental or unwitting use results in circumvention. Nor does it bar those devices (etc.) that, while capable of, and even used for, circumvention, are primarily designed or used for other purposes. The law prohibits the manufacture, etc. of devices, services, etc., only in the following three circumstances:

(A) The device (etc.) was "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access" to a copyrighted work; or

(B) The device (etc.) was not primarily designed to circumvent, but in fact "has only limited commercially significant purpose or use other than to circumvent ..."; or

(C) The device (etc.) is "marketed" (i.e., advertised or promoted) as a device (etc.) to be used to circumvent access controls. In this case, the target of the law is the person promoting the circumventing use; it is not the manufacturer (etc.) of the device (etc.), unless that person acts in concert with the marketer.

…

e. §1201(b): Circumvention of technological protections of (traditional) rights under copyright

The DMCA also addresses technological protection of the post-access rights of reproduction, adaptation, distribution, public performance or display. Here, the bill addresses only the producers and suppliers of circumvention devices, services (etc.); the end-user's activities are not at issue. As with section 1201(a), section 1201(b) does not target all devices (etc.) that are capable of being used for circumvention. Manufacture and distribution of post-access circumvention devices, services (etc.) are prohibited only if (A) they are "primarily designed" to circumvent; or (B) if they have "only limited commercially significant" uses other than to circumvent; or (C) if they are "marketed" as circumvention devices.

The prohibition contained in this subsection is not as stringent as that of the subsection concerning access controls. The post-access devices (etc.) here targeted are those that circumvent "protection afforded by a technological measure that effectively protects a right of a copyright owner under this title ...." The exclusive rights under copyright set forth in section 106 of the Copyright Act are expressly made "subject to sections 107 through 120," sections that set forth a variety of exceptions to and limitations on copyright (referred to collectively as "fair uses"). If the circumvention device (etc.) is designed for or can be put to commercially significant fair use, then it is not a violation of §1201(b) to sell the device or to offer the circumvention service. Here, as in the case of circumventions of access controls, however, the device itself probably cannot distinguish between circumventions for fair use purposes, and circumventions aimed simply at obtaining unauthorized copies. But were the device exculpated simply because it is capable of being put to fair use, then, as a practical matter, the fair use tail would again wag the copyright infringement dog.

Nonetheless, this need not mean that there can be no manufacture and distribution of circumvention devices (etc.). The lawfulness of the manufacture and distribution should turn on the definition of the market for the device or service (etc.). A copy protection-defeating device addressed to the general public may not be likely to have commercially significant fair uses; one created for or disseminated to a community of researchers and scholars is a better candidate.

Put another way, so long as university or library personnel employ circumvention devices or services that they have devised (or that are created at the library or university's behest), and so long as the devices or services are used to make copies (or adaptations, distributions, public performances or displays) that would qualify as fair uses, there should be no violation of section 1201(b).

There is at least one major objection to this market-based analysis: it appears to privilege formal fair use communities, such as universities and libraries, over the general public (although all members of the public can be library users). All members of the public are entitled to invoke the fair use exception (in appropriate circumstances). Non-scholarly fair use can include parody and other forms of commentary. Under Sony Corp. of America v. Universal City Studios, Inc., some kinds of temporary noncommercial copying for personal convenience may also be fair use. If one assumes that technological measures will accompany all copies of the works targeted for parody, or for private copying, then how will the user (who is insufficiently computer-adept to do the circumvention herself) be able to obtain and exercise the means to make the further copies necessary to carry out her fair use project? The assumption that copyright owners will only make their works available in copy-protected form may well be overstated; nonetheless this is one issue that Congress instructed the Copyright Office to take into account in preparing its study of the "impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research ...."

B. DMCA Exceptions

Section 1201(a)(1) of the DMCA codifies a new set of legal entitlements (and corresponding burdens) regarding systems that might protect copyrighted content. These are distinct from the basic entitlements con-

ferred by copyright law itself. For example, U.S. copyright law does not preserve for copyright holders a default right to control access to copies of their works once distributed. Opening a book and reading it is not an event of legal moment as far as Title 17 is concerned, and lending such a book is explicitly protected against a claim of infringement by the First Sale Doctrine, 17 U.S.C. 109. Thus can libraries exist, even if their lending of books can be demonstrated to harm the market for them. (After all, many people who borrow a book might otherwise have bought it.)

The fact that the anti-circumvention provisions are separate from underlying copyright law does not simply mean that actions previously innocuous are now penalized. In addition, actions previously privileged under copyright law may become much more difficult. To understand this, consider again the First Sale Doctrine. So long as one has a book, one can lend it, and a copyright suit challenging the lending will be open and shut thanks to an invocation of 17 U.S.C. 109's First Sale defense. Now imagine an electronic book registered to a single desktop computer. One may wish to lend the book to a friend – making the book disappear from her computer and appear on the friend's instead, perhaps thanks to having been attached to an email. But a trusted system might flatly prohibit such a use, or require additional payment before allowing it. These prohibitions, written into the code, cannot be ignored. The First Sale Doctrine is only a defense to copyright infringement – it, like other defenses such as fair use, is not a right. So one cannot demand that the company allow the lending of one's electronic book, even though if one could figure out how to make such lending take place, the lending would not itself be subject to a claim of copyright infringement. (The right to demand that one not be technologically barred from activities that would be privileged as fair use or under the first sale doctrine might be thought of as "copyduty," something that does not exist in Title 17.)

Notes and Questions

1) Suppose that Dorothy buys a CD from her local music store. (There is no license involved – this is a simple purchase.) She enjoys the music a great deal and decides to share it with her friend, Ian. Dorothy lends the CD to Ian, but is frustrated to learn that the CD will not play on his computer. Dorothy next learns that her CD employs the latest in anti-piracy technology; once she played the CD on her computer, it was registered to her computer and rendered inoperable on any other machine.

Vaguely familiar with the First Sale Doctrine – and profoundly irate – Dorothy plans to sue the record company that holds the copyrights in her CD in order to compel them to allow her to share her CD with Ian. Does she have a valid claim? Would your answer be any different if Ian's use of the CD was defensible – with respect to the claim of copyright infringement – on the basis of fair use?

2) Now suppose that Ian – a gifted computer scientist – cracks the anti-piracy technology that locks the content on Dorothy's CD. Can he be prosecuted under the DMCA? Does he have a defense under the First Sale Doctrine? What if his use of the CD is a fair use?

* * *

Perhaps, then, the defenses to claims of copyright infringement such as "fair use" or "first sale" presuppose – now wrongly – that the users can gain access to the work to engage in such activity in the first instance.

While the DMCA proclaims in § 1201(c)(1) that "nothing in [§ 1201] shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under [Title 17]", its framers were nonetheless acutely aware of the potential danger that § 1201(a)(1) could effectively eliminate fair use by barring access. For this reason, they constructed several exceptions to § 1201(a)(1).

Sections 1201(a)(1)(B) and (C) most directly address the concerns described above:

> (B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibi-

tion in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine –

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrightedworks has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

On October 27, 2000, the Librarian of Congress published in the Federal Register a rule implementing subsection (C):

Federal Register: October 27, 2000 (Volume 65, Number 209)
Rules and Regulations

Page 64555-64574

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

AGENCY: Copyright Office, Library of Congress.

ACTION: Final Rule.

Library of Congress, Copyright Office, 37 CFR Part 201, [Docket No. RM 99-7D]

II. Solicitation of Public Comments and Hearings

On November 24, 1999, the Office initiated the rulemaking procedure with publication of a Notice of Inquiry. 64 FR 66139. The Notice of Inquiry requested written comments from all interested parties, including representatives of copyright owners, educational institutions, libraries and archives, scholars, researchers and members of the public. The Office devoted a great deal of attention in this Notice to setting out the legislative parameters and developing questions related to the criteria Congress had established. ...

In response to the Notice of Inquiry, the Office received 235 initial comments and 129 reply comments. Thirty-four witnesses representing over 50 groups testified at five days of hearings held in either Washington, DC or Palo Alto, California. The Office placed all initial comments, reply comments, optional written statements of the witnesses and the transcripts of the two hearings on its website shortly after their receipt. Following the hearings, the Office received 28 post-hearing comments, which were also posted on the website. All of

these commenters and witnesses are identified in the indexes that appear on the Office's website.

...

III. Discussion

...

C. Conclusions Regarding This Rulemaking and Summary of Recommendations

After reviewing all of the comments and the testimony of the witnesses who appeared at the hearings, the Register concludes that a case has been made for exemptions relating to two classes of works:

(1) Compilations consisting of lists of websites blocked by filtering software applications; and

(2) Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness.

These recommendations may seem modest in light of the sweeping exemptions proposed by many commenters and witnesses, but they are based on a careful review of the record and an application of the standards governing this rulemaking procedure. While many commenters and witnesses made eloquent policy arguments in support of exemptions for certain types of works or certain uses of works, such arguments in most cases are more appropriately directed to the legislator rather than to the regulator who is operating under the constraints imposed by section 1201(a)(1).

Many of the proposed classes do not qualify for exemption because they are not true ``classes of works'' as described above in section III.A.3. The proposed exemptions discussed below in section III.E.2, 5, 6, 7, 8, and 9 all suffer from that frailty to varying degrees. In many cases, proponents attempted to define classes of works by reference to the intended uses to be made of the works, or the intended user. These criteria do not define a ``particular class of copyrighted work.''

...

Dated: October 23, 2000.

James H. Billington,

The Librarian of Congress

The librarians' exception: 17 U.S.C. 1201(d)

(d) Exemption for nonprofit libraries, archives, and educational institutions.

(1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph —

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1) —

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be —

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

Jane C. Ginsburg

Copyright Legislation for the Digital Millenium

23 Colum.-VLA J.L. & Arts 137

d. §1201[(e)]-(j): Exceptions to protection against circumvention of access controls

…

ii. §1201(e): Law enforcement; §1201(j): Security testing

Section 1201(e) entitles federal, state and local law enforcement officers to defeat access controls in order to conduct an authorized investigation. The investigation may extend to verifying "information security," defined as "activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network." Similarly, §1201(j) permits circumvention for purposes of "security testing," defined as "good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." These provisions are not intended to serve as licenses to "hack" into a computer system. The persons verifying a system's security must be either law enforcement officers, or persons authorized by the computer system owner or operator to conduct the test. The exception does not exempt the technologically adept who unilaterally do owners or operators the "favor" of breaking into their systems in order to warn them of the systems' vulnerabilities.

iii. §1201(f): Reverse engineering

This provision addresses decompilation of computer programs to achieve interoperability. It permits persons who have "lawfully obtained the right to use a copy" of a computer program to defeat the access code (either directly or by "developing and employing" a circumvention device) "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs ...." … The concern underlying this provision was that software producers would defeat decompilation by issuing computer programs only in access-protected forms. Because access protection is distinct from copyright infringement, §1201 in its original form would have prevented the circumvention of an access code even if the purpose of the circumvention was to perform an act that courts had ruled could be fair use. …

Could Ed Felton, see <X>, use this exception?

iv. §1201(g): Encryption research

This provision … defines encryption research as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if

these activities are conducted to advance the state of knowledge in the field of encryption ...," and permits specified users to circumvent (and to "develop and employ" circumvention devices) for this "sole purpose." This provision also imposes detailed limitations on the would-be encryption researcher: the encrypted copy must be "lawfully obtained"; defeating the access code must be "necessary to conduct such encryption research"; the researcher must have made a "good faith effort to obtain authorization"; and the "act of good faith encryption research" must "not constitute infringement under this title or a violation of applicable law other than this section ...." Out of apparent concern that "encryption research" could degenerate into a pretext for indiscriminate hacking of access controls, this provision further attempts to restrict the class of persons qualified for the exemption by listing factors to consider: whether the information derived from the research was disseminated in a manner "reasonably calculated to advance the state of knowledge or development of encryption technology" or whether instead it "facilitates infringement"; whether the person "is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology"; and whether and when the results of the research are disclosed to the copyright owner. …

v. §1201(h): "Exceptions Regarding Minors"

This provision addresses the concerns of parents who seek to prevent their children from seeing inappropriate material on the Internet. Congress was persuaded that screening devices that parents would employ to protect their children might include a "component or part" that circumvents access controls, but that these devices should be available if the "component or part" is necessary to a device that "does not itself violate the provisions of this title" and has the "sole purpose to prevent the access of minors to material on the Internet."

…

vi. §1201(i): Protection of personally identifying information

This provision responds to significant privacy concerns raised by users of digital networks. Some website operators have, without notifying users, engaged in the practice of collecting or disseminating information about the online activities of persons who contact the websites, for example, by sending "cookies" to the user's hard drive. This exception therefore permits users to circumvent an access control in order to discover and disable an undisclosed information-gathering feature. If, by contrast, the information-gatherer provides "conspicuous notice" of its information collection, and enables the user to restrict the collection or dissemination of personally identifying information, then the user may not circumvent. [FN40] Similarly, the right to circumvent is limited to identifying and disabling the undisclosed "cookie" or similar device; it does not entitle the user to "gain access to any work."

As this survey demonstrates, §1201's panoply of exceptions presents something of a grab-bag; it is difficult to discern from the various exceptions an overall legislative policy regarding the kinds of access control circumventions that should offset copyright owners' enhanced ability to control the use of their works. From the user's perspective, the proliferation of narrow exceptions prompts the negative inference that any circumvention not expressly exempted is prohibited. Far from promoting a flexible, fair use-like approach to the circumvention of access controls, the overspecification of special exemptions may well make it more difficult to articulate a general user privilege supporting circumvention of access controls.

Arguably, §1201(c) accords courts residual authority to expand exceptions to access control. That provision specifies that nothing in §1201 affects "defenses to copyright infringement, including fair use, under this title." One might object that a violation of §1201(a) is not copyright infringement, it is a new violation for which the DMCA provides distinct remedies.

Nonetheless, circumvention claims remain copyright-dependent, since §1201(a) covers only measures that protect access to copyrighted works. …

C. DeCSS and other disputes refining the scope of the DMCA

Universal City Studios, Inc. v. Corley

273 F.3d 429 (2nd Cir. 2001)

Jon O. Newman, Circuit Judge.

Introduction

…

This appeal concerns the anti-trafficking provisions of the DMCA, which Congress enacted in 1998 to strengthen copyright protection in the digital age. Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections. In so doing, Congress targeted not only those pirates who would *circumvent* these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201(a)(1)), but also anyone who would *traffic* in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. § 1201(a)(2), (b)(1)).

…

Background

… In the early 1990s, [motion picture] studios began to consider the possibility of distributing movies in digital form as well. Movies in digital form are placed on disks, known as DVDs, which can be played on a DVD player (either a stand-alone device or a component of a computer). DVDs offer advantages over analog tapes, such as improved visual and audio quality, larger data capacity, and greater durability. However, the improved quality of a movie in a digital format brings with it the risk that a virtually perfect copy, *i.e.,* one that will not lose perceptible quality in the copying process, can be readily made at the click of a computer control and instantly distributed to countless recipients throughout the world over the Internet. This case arises out of the movie industry's efforts to respond to this risk by invoking the anti-trafficking provisions of the DMCA.

I. CSS

The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as

Note the use of contract here to make sure there is no race to the bottom among consumer device manufacturers. If a manufacturer did not agree to build certain limits into its DVD player, it would not be entitled to a CSS key from the industry administrative association, and thus could not build a player to play DVDs. Prior to the DMCA, what would have happened if a manufacturer had simply cracked CSS and built a functioning multi-featured DVD player without having signed the license?

well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. Player keys and other information necessary to the CSS scheme were given to manufacturers of DVD players for an administrative fee. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required in the licensing agreement to prevent the transmission of "CSS data" (a term undefined in the licensing agreement) from a DVD drive to any "internal recording device," including, presumably, a computer hard drive.

With encryption technology and licensing agreements in hand, the studios began releasing movies on DVDs in 1997, and DVDs quickly gained in popularity, becoming a significant source of studio revenue. In 1998, the studios secured added protection against DVD piracy when Congress passed the DMCA, which prohibits the development or use of technology designed to circumvent a technological protection measure, such as CSS. The pertinent provisions of the DMCA are examined in greater detail below.

II. DeCSS

In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS."

If a user runs the DeCSS program (for example, by clicking on the DeCSS icon on a Microsoft operating system platform) with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-CSS-compliant player and copied, manipulated, and transferred just like any other computer file. DeCSS comes complete with a fairly user-friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. *Universal I*, 111 F.Supp.2d at 308, 313. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).

Johansen posted the executable object code, but not the source code, for DeCSS on his web site. … Within months of its appearance in executable form on Johansen's web site, DeCSS was widely available on the Internet, in both object code and various forms of source code. *See* Trial Exhibit CCN (Touretzky Article: *Gallery of CSS Descramblers*).

In November 1999, Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, *2600: The Hacker Quarterly,* which Corley has been publishing since 1984. As the name suggests, the magazine is designed for "hackers," as is the web site. While the magazine and the web site cover some issues of general interest to computer users—such as threats to online privacy—the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to circumvent the security systems. Representative

articles explain how to steal an Internet domain name and how to break into the computer systems at Federal Express. *Universal I*, 111 F.Supp.2d at 308-09.

Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, ... [y]ou have to show your evidence ... and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence ... we have" that there is in fact technology that circumvents CSS. Trial Tr. at 823. Writing about DeCSS without including the DeCSS code would have been, to Corley, "analogous to printing a story about a picture and not printing the picture." *Id.* at 825. Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found. *Id.* at 791, 826, 827, 848.

2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease- and-desist letters to many of these sites. These efforts met with only partial success; a number of sites refused to remove DeCSS. In January 2000, the studios filed this lawsuit.

III. The DMCA

The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty"), which requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." WIPO Treaty, Apr. 12, 1997, art. 11, S. Treaty Doc. No. 105-17 (1997), available at 1997 WL 447232. Even before the treaty, Congress had been devoting attention to the problems faced by copyright enforcement in the digital age. Hearings on the topic have spanned several years. … This legislative effort resulted in the DMCA.

The Act contains three provisions targeted at the circumvention of technological protections. The first is subsection 1201(a)(1)(A), the anti-circumvention provision. This provision prohibits a person from "circumvent[ing] a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]." The Librarian of Congress is required to promulgate regulations every three years exempting from this subsection individuals who would otherwise be "adversely affected" in "their ability to make noninfringing uses." 17 U.S.C. § 1201(a)(1)(B)-(E).

The second and third provisions are subsections 1201(a)(2) and 1201(b)(1), the "anti-trafficking provisions." Subsection 1201(a)(2), the provision at issue in this case, provides:

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure *441 that effectively controls access to a work protected under this title.

Id. § 1201(a)(2). To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work ... or otherwise to ... bypass ... a technological measure, without the authority of the copyright owner." *Id.* § 1201(a)(3)(A).

Subsection 1201(b)(1) is similar to subsection 1201(a)(2), except that subsection 1201(a)(2) covers those who traffic in technology that can circumvent "a technological measure *that effectively controls access* to a work protected under" Title 17, whereas subsection 1201(b)(1) covers those who traffic in technology that can circumvent "protection afforded by a technological measure *that effectively protects a right of a copyright owner* under" Title 17. *Id.* § 1201(a)(2), (b)(1) (emphases added). In other words, although both subsections prohibit trafficking in a circumvention technology, the focus of subsection 1201(a)(2) is circumvention of technologies designed to *prevent access* to a work, and the focus of subsection 1201(b)(1) is circumvention of technologies designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright. *See* S.Rep. No. 105-190, at 11-12 (1998). Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology.

…

The DMCA creates civil remedies, *id.* § 1203, and criminal sanctions, *id.* § 1204. It specifically authorizes a court to "grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation." *Id.* § 1203(b)(1).

IV. Procedural History

Invoking subsection 1203(b)(1), the Plaintiffs sought an injunction against the Defendants, alleging that the Defendants violated the anti- trafficking provisions of the statute. On January 20, 2000, after a hearing, the District Court issued a preliminary injunction barring the Defendants from posting DeCSS. *Universal City Studios, Inc. v. Reimerdes*, 82 F.Supp.2d 211 (S.D.N.Y.2000).

The Defendants complied with the preliminary injunction, but continued to post links to other web sites carrying DeCSS, an action they termed "electronic civil disobedience." *Universal I*, 111 F.Supp.2d at 303, 312. Under the heading "Stop the MPAA [(Motion Picture Association of America)]," Corley urged other web sites to post DeCSS lest "we ... be forced into submission." *Id.* at 313.

The Plaintiffs then sought a permanent injunction barring the Defendants from both posting DeCSS and linking to sites containing DeCSS. After a trial on the merits, the Court issued a comprehensive opinion, *Universal I*, and granted a permanent injunction, *Universal II*.

The Court explained that the Defendants' posting of DeCSS on their web site clearly falls within section 1201(a)(2)(A) of the DMCA, rejecting as spurious their claim that CSS is not a technological measure that "effectively controls access to a work" because it was so easily penetrated by Johansen, *Universal I*, 111 F.Supp.2d at 318, and as irrelevant their contention that DeCSS was designed to create a Linux-platform DVD player, *id.* at 319. The Court also held that the Defendants cannot avail themselves of any of the DMCA's exceptions, *id.* at 319-22, and that the alleged importance of DeCSS to certain fair uses of encrypted copyrighted material was immaterial to their statutory liability, *id.* at 322-24. The Court went on to hold that when the Defendants "proclaimed on their own site that DeCSS could be had by clicking on the hyperlinks" on their site, they were trafficking in DeCSS, and therefore liable for their linking as well as their posting. *Id.* at 325.

[The trial court rejected defendant's arguments challenging the constitutionality of the DMCA as applied.]

Finally, the Court concluded that an injunction was highly appropriate in this case. …

The Court's injunction barred the Defendants from: "posting on any Internet web site" DeCSS; "in any other way ... offering to the public, providing, or otherwise trafficking in DeCSS"; violating the anti-trafficking provisions of the DMCA in any other manner, and finally "knowingly linking any Internet web site operated by them to any other web site containing DeCSS, or knowingly maintaining any such link, for the purpose of disseminating DeCSS." *Universal II*, 111 F.Supp.2d at 346-47.

The Appellants have appealed from the permanent injunction. …

What is the purpose behind 1201(c)(1) in the view of the court? In your view?

Discussion

I. Narrow Construction to Avoid Constitutional Doubt

The Appellants first argue that, because their [First Amendment] arguments are at least substantial, we should interpret the statute narrowly so as to avoid constitutional problems. They identify three different instances of alleged ambiguity in the statute that they claim provide an opportunity for such a narrow interpretation.

First, they contend that subsection 1201(c)(1), which provides that "[n]othing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title," can be read to allow the circumvention of encryption technology protecting copyrighted material when the material will be put to "fair uses" exempt from copyright liability. We disagree that subsection 1201(c)(1) permits such a reading. Instead, it clearly and simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred. …

Second, the Appellants urge a narrow construction of the DMCA because of subsection 1201(c)(4), which provides that "[n]othing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products." This language is clearly precatory: Congress could not "diminish" constitutional rights of free speech even if it wished to, and the fact that Congress also expressed a reluctance to "enlarge" those rights cuts against the Appellants' effort to infer a narrowing construction of the Act from this provision.

Third, the Appellants argue that an individual who buys a DVD has the "authority of the copyright owner" to view the DVD, and therefore is exempted from the DMCA pursuant to subsection 1201(a)(3)(A) when the buyer circumvents an encryption technology in order to view the DVD on a competing platform (such as Linux). The basic flaw in this argument is that it misreads subsection 1201(a)(3)(A). That provision exempts from liability those who would "decrypt" an encrypted DVD with the authority of a copyright owner, not those who would "view" a DVD with the authority of a copyright owner. In any event, the Defendants offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms.

We conclude that the anti-trafficking and anti-circumvention provisions of the DMCA are not susceptible to the narrow interpretations urged by the Appellants. We therefore proceed to consider the Appellants' constitutional claims.

II. Constitutional Challenge Based on the Copyright Clause

[The Court refuses to fully entertain this challenge on the grounds that it was improperly raised in a footnote and is wholly "premature and speculative."]

III. Constitutional Challenges Based on the First Amendment

[The Court extensively discusses the "applicable principles" governing its First Amendment analysis of legislation restricting software: i) Code as Speech, ii) Computer Programs as Speech, iii) The Scope of First Amendment Protection for Computer Code, and iv) The Scope of First Amendment Protection for Decryption Code. It then considers defendant's specific First Amendment challenges.]

…

Our task is to determine whether the legislative solution adopted by Congress, as applied to the Appellants by the District Court's injunction, is consistent with the limitations of the First Amendment, and we are satisfied that it is.

IV. Constitutional Challenge Based on Claimed Restriction of Fair Use

Asserting that fair use "is rooted in and required by both the Copyright Clause and the First Amendment," Brief for Appellants at 42, the Appellants contend that the DMCA, as applied by the District Court, unconstitutionally "*eliminates* fair use" of copyrighted materials, *id.* at 41 (emphasis added). We reject this extravagant claim.

Preliminarily, we note that the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might arguably be enlisted for such a requirement. …

We need not explore the extent to which fair use might have constitutional protection, grounded on either the First Amendment or the Copyright Clause, because whatever validity a constitutional claim might have as to an application of the DMCA that impairs fair use of copyrighted materials, such matters are far beyond the scope of this lawsuit for several reasons.

Second, as the District Court properly noted, to whatever extent the anti-trafficking provisions of the DMCA might prevent others from copying portions of DVD movies in order to make fair use of them, "the evidence as to the impact of the anti-trafficking provisions of the DMCA on prospective fair users is scanty and fails adequately to address the issues." Universal I, 111 F. Supp. 2d at 338 n.246.

Third, the Appellants have provided no support for their premise that fair use of DVD movies is constitutionally required to be made by copying the original work in its original format. Their examples of the fair uses that they believe others will be prevented from making all involve copying in a digital format those portions of a DVD movie amenable to fair use, a copying that would enable the fair user to manipulate the digitally copied portions. One example is that of a school child who wishes to copy images from a DVD movie to insert into the student's documentary film. We know of no authority for the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original. Although the Appellants insisted at oral argument that they should not be relegated to a "horse and buggy" technique in making fair use of DVD movies, the DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses of DVD movies, such as commenting on their content, quoting excerpts from their screenplays, and even recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie. The fact that the resulting copy will not be as perfect or as manipulable as a digital copy obtained by having direct access to the DVD movie in its digital form, provides no basis for a claim of unconstitutional limitation of fair use. A film critic making fair use of a movie by quoting selected lines of dialogue has no constitutionally valid claim that the review (in print or on television) would be technologically superior if the reviewer had not been prevented from using a movie camera in the theater, nor has an art student a valid constitutional claim to fair use of a painting by photographing it in a museum. Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original.

Conclusion

We have considered all the other arguments of the Appellants and conclude that they provide no basis for disturbing the District Court's judgment. Accordingly, the judgment is affirmed.

Notes and Questions: The Significance of DeCSS

1) Judge Newman, writing for the Second Circuit in *Universal v. Corley*, explains that movie studios license the CSS technology required to unscramble DVD content – most fundamentally, the decryption keys – to DVD player manufacturers (whether hardware or software). This is accomplished through the DVD Copy Control Association ("DVDCCA"), a trade association of businesses in the movie industry that controls the rights to CSS. It is important to stress that, through CSS, the DVDCCA is able to force player manufacturers to submit to the terms and conditions of its licenses. CSS not only affords the movie industry copyright protection from end users, but also leverage over the manufacturers of players. Under the terms of its CSS license, the DVDCCA can control the extent and nature of the functionality offered to end users of DVD players.

2) The availability of DeCSS not only strips the movie industry of its copyright protection from end users, but also, in theory, eliminates its leverage over DVD player manufacturers. Were it not for the DMCA, the manufacturer of a DVD player could use DeCSS to unscramble DVDs, eliminating the need to submit to the terms of the DVDCCA's license for the CSS technology.

CSS, then, is a technology that works in tandem with private law (contract) to provide control over digital intellectual property. Largely the result of efforts by a trade association similar to the DVDCCA, the Audio Home Recording Act ("AHRA") represents a similar pairing of law and technology. The AHRA is, naturally, public law and the relationship between the AHRA and the associated technologies is inverted; the AHRA mandates compliance with certain technology specifications while CSS is a private technology that forces companies to submit to private law (that is, forces player manufacturers to submit to the terms of CSS technology licenses). We will further explore the AHRA, and this theme of resonance with the DeCSS controversy, later in this chapter.

While the DMCA provides for monetary damages, most disputes have centered on prayers for injunctive relief. Defendants are often judgment-proof and plaintiffs most often seek, above all else, to stem the distribution of circumvention technologies. Once unleashed, a program like DeCSS, for example, is guaranteed to spring up in thousands of places, in hundreds of different forms. Once this occurs, an action against the original "manufacturer" of the circumvention device alone can be meaningless; in order to limit the distribution of the program, the injured party must rely on actions against those "trafficking" in the circumvention technology. Given the Internet's vast scale and the ease of distribution on the Internet, such a campaign can resemble the challenge of putting the proverbial genie back in the lamp. Pursuing every possible defendant – every site from which an internet user can gain access to a circumvention tool – is often prohibitively costly.

3) A more fundamental challenge lies in the inherent scope of the DMCA. What behavior constitutes "trafficking?" This question was central to the DeCSS dispute. Specifically, does 2600.com violate the DMCA merely by linking to sites that offer DeCSS? As explained by Judge Kaplan, writing for the U.S. District Court for the Southern District of New York:

Universal City Studios Inc. v. Reimerdes

111 F. Supp. 2d 294 (S.D. N.Y. 2000), 324-35

> Plaintiffs seek also to enjoin defendants from "linking" their 2600.com web site to other sites that make DeCSS available to users. Their request obviously stems in no small part from what defendants themselves have termed their act of "electronic civil disobedience" —their attempt to defeat the purpose of the preliminary injunction by (a) offering the practical equivalent of making DeCSS available on their own web site by electronically linking users to other sites still offering DeCSS, and (b) encouraging other sites that had not been enjoined to offer the program. The dispositive question is whether linking to another web site containing DeCSS constitutes "offering [DeCSS] to the public" or "providing or otherwise trafficking" in it within the meaning of the DMCA. Answering this question requires careful consideration of the nature and types of linking.

> ...
>
> As noted earlier, the links that defendants established on their web site are of several types. Some transfer the user to a web page on an outside site that contains a good deal of information of various types, does not itself contain a link to DeCSS, but that links, either directly or via a series of other pages, to another page on the same site that posts the software. It then is up to the user to follow the link or series of links on the linked-to web site in order to arrive at the page with the DeCSS link and commence the download of the software. Others take the user to a page on an outside web site on which there appears a direct link to the DeCSS software and which may or may not contain text or links other than the DeCSS link. The user has only to click on the DeCSS link to commence the download. Still others may directly transfer the user to a file on the linked-to web site such that the download of DeCSS to the user's computer automatically commences without further user intervention.
>
> ...
>
> To the extent that defendants have linked to sites that automatically commence the process of downloading DeCSS upon a user being transferred by defendants' hyperlinks, there can be no serious question. Defendants are engaged in the functional equivalent of transferring the DeCSS code to the user themselves.
>
> Substantially the same is true of defendants' hyperlinks to web pages that display nothing more than the DeCSS code or present the user only with the choice of commencing a download of DeCSS and no other content. The only distinction is that the entity extending to the user the option of downloading the program is the transferee site rather than defendants, a distinction without a difference.
>
> Potentially more troublesome might be links to pages that offer a good deal of content other than DeCSS but that offer a hyperlink for downloading, or transferring to a page for downloading, DeCSS. If one assumed, for the purposes of argument, that the Los Angeles Times web site somewhere contained the DeCSS code, it would be wrong to say that anyone who linked to the Los Angeles Times web site, regardless of purpose or the manner in which the link was described, thereby offered, provided or otherwise trafficked in DeCSS merely because DeCSS happened to be available on a site to which one linked. But that is not this case. Defendants urged others to post DeCSS in an effort to disseminate DeCSS and to inform defendants that they were doing so. Defendants then linked their site to those "mirror" sites, after first checking to ensure that the mirror sites in fact were posting DeCSS or something that looked like it, and proclaimed on their own site that DeCSS could be had by clicking on the hyperlinks on defendants' site. By doing so, they offered, provided or otherwise trafficked in DeCSS, and they continue to do so to this day.

Forced to draw a line between lawful behavior and trafficking, Judge Kaplan drew the line he found most sensible. Do you agree with his analysis? Why or why not? As a result of Judge Kaplan's order, 2600.com simply made its links to sites offering DeCSS "inoperable," but continues to offer a text list of the associated URLs (not "clickable" links). In order to access a listed site, a user must copy its URL, presented only as text, and paste the URL into the address bar of his or her browser. As explained by 2600.com:

> The MPAA has succeeded in getting an injunction against us to remove any links to sites with DeCSS. Therefore, you can no longer click on the sites below to get to the DeCSS utility. Of course, you can always go to Disney's search engine and search for DeCSS. They will then LINK you to thousands of sites, something we're no loner allowed to do.

(Posted at: http://www.2600.com/news/1227-help.html.)

Posting URLs in text form is almost certainly lawful; 2600.com now only contains "descriptive text" explaining where a user can find DeCSS. Does this change your view of Judge Kaplan's opinion or the larger dispute?

3) A third problem for those seeking relief under the DMCA lies in the limited reach of a court. This issue was central to the dispute over "CPHack," a program designed to circumvent the decryption technology

deployed in Mattel's CyberPatrol filtering software. CyberPatrol is a commercial software application that can be used to block access to websites that contain various forms of "harmful" content. Parents, for example, can use CyberPatrol to prevent their children from accessing websites that contain pornography or violence. At its core, CyberPatrol is essentially a proprietary blacklist; the application is most fundamentally a database of websites and associated categorizations of their content. The makers of the software used an encryption scheme to keep secret the contents of the blacklist. In March of 2000, Eddy Jansson of Sweden and Matthew Skala of Canada published a report entitled "*The Breaking of Cyber Patrol® 4*" in which they documented a technique for circumventing CyberPatrol's encryption scheme and made available the "CPHack" application. Using CPHack, CyberPatrol 4 users can load and browse CyberPatrol 4's blacklist. (Jannson and Skala claim that their purpose for cracking the list was to expose any hidden agenda CyberPatrol might have in compiling the blacklist and to fuel widespread criticism about filtering programs – or "Censorware" – in general.) Janson and Skala invited visitors to their site to freely copy and distribute their CPHack application.

Mattel and Microsystems Software, the developer of CyberPatrol, brought suit under the DMCA. (Mattel and Microsystems maintain copyright interests in their blacklist. CPHack, then, is an application that "circumvent[s] a technological measure that effectively controls access to a work protected [by copyright]." 17 U.S.C. 1201(a)(1)(A).) After much dispute, the parties reached an agreement and Judge Harrington, writing for the U.S. District Court for the District of Massachusetts, entered a "Stipulated Permanent Injunction." 98 F. Supp. 2d 74 (D. Mass. 2000).

The remainder of the dispute centered on the reach of Judge Harrington's order. Judge Harrington was deeply troubled by CPHack. In his three page order, he writes:

> Yet this case involves more than a complex and significant legal issue relating to copyright law. It raises a most profound societal issue, namely, who is to control the educational and intellectual nourishment of young children - the parents or the purveyors of pornography and the merchants of death and violence.
>
> Ideas bear consequences, fruitful and also destructive. The pernicious idea that all men are not created equal is the philosophic basis which incited the degradations of slavery and the genocidal slaughter of the Holocaust.
>
> Under our Constitution all have the right to disseminate even evil ideas and such ideas cannot by law be suppressed by the government. On the other hand, parents, in the exercise of their parental obligation to educate their young children, have the equal right to screen and, thus, prevent noxious and insidious ideas from corrupting their children's fertile and formative minds.

Id. at 74-75. It is clear that Judge Harrington intended for his order to apply to all sites mirroring the CPHack paper and application. It states: "Defendants Jansson and Skala, their agents, employees, and all persons in active concert or participation with Defendant Jansson and/or Defendant Skala, shall discontinue and be permanently enjoined from publishing the software source code and binaries known as 'CP4break.zip' or 'cphack.exe' or any derivative thereof." Id. at 74. Claiming victory, attorneys for Mattel and Microsystems began contacting the myriad sites offering the CPHack application, demanding that the sites' proprietors comply with the order. In some cases, subpoenas were sent via email. Commentators termed these communications "spampoenas." (Harrington's order requires service by certified mail. Id.)

A fundamental question arose: Could Judge Harrington's order reach all sites hosting a copy of the CPHack application? To the extent that meaningful relief requires stemming the distribution of a circumvention device, those that seek relief under the DMCA would argue that it should. Clearly, though, notions of due process are implicated by such a wide-ranging order; a proprietor of a website must have his / her day in court before being permanently enjoined. The U.S. Court of Appeals for the First Circuit considered this issue when it reviewed Judge Harrington's denial of a motion to appeal his contempt order by three mirror sites that were not parties to the dispute. 226 F.3d 35 (1st Cir. 2000). Judge Selya writes for that court:

> The named defendants stipulated to the entry of the injunction, but three nonparties — Waldo Jaquith, Lindsay Haisley, and Bennett Haselton — now attempt to appeal. They claim to have copied the proscribed code from the named defendants' web pages and assert that the injunction impermissibly interferes with their right to continue posting it on their "mirror sites."

> …
>
> [M]ere participation in the proceedings below will not suffice to confer standing upon a nonparty. Thus, we reject the appellants' claim that participation below, even if coupled with an indirect interest in the judgment sought to be appealed, confers standing.
>
> Ably represented, the appellants take yet another tack. They remonstrate that if they are not permitted to appeal at this juncture, they will forfeit any opportunity to contest the injunction on the merits. In their view, this would deprive them of due process.
>
> …
>
> … [T]he adjudicative framework surrounding contempt proceedings fully protects nonparties' constitutional rights. If contempt proceedings are in fact undertaken, the forum court will resolve the fact-specific question of whether the cited nonparty was in active concert or participation with the named defendant. If so, the named defendant will be deemed the nonparty's agent, and the nonparty's right to due process will have been satisfied vicariously. See Merriam, 639 F.2d at 35; Alemite Mfg. Corp. v. Staff, 42 F.2d 832, 832-33 (2d Cir. 1930) (L. Hand, J.). If, however, the party prosecuting the contempt proceeding fails to show active concert or participation, a finding of contempt will not lie. See Zenith Radio Corp. v. Hazeltine Research, Inc., 395 U.S. 100, 112, 23 L. Ed. 2d 129, 89 S. Ct. 1562 (1969); Merriam, 639 F.2d at 35.
>
> …
>
> The coin, however, has a flip side. A nonparty who has acted independently of the enjoined defendant will not be bound by the injunction, and, if she has had no opportunity to contest its validity, cannot be found in contempt without a separate adjudication. See id.; see also Alemite, 42 F.2d at 832 (declaring that a decree which purports to enjoin nonparties who are neither abettors nor legally identified with the defendant "is pro tanto brutum fulmen," and may safely be ignored). This tried and true dichotomy safeguards the rights of those who truly are strangers to an injunctive decree. It does not offend due process.

Id. at 37, 42-43. While Judge Selya's opinion ably resolves the legal issues at stake, the more fundamental question remains unresolved: Is a website that hosts a copy of CPHack "in active concert or participation" with the named defendants in the dispute? How should this question be answered? Can you make compelling arguments for both a narrow and broad reach for Judge Harrington's order? How does the First Amendment, and our discussion of code as speech, bear on this question?

RealNetworks v. Streambox

2000 U.S. Dist. LEXIS 1889

United States District Court for the Western District of Washington

Pechman, Marsha J.

Introduction

Plaintiff RealNetworks, Inc. ("RealNetworks") filed this action on December 21, 1999. RealNetworks claims that Defendant Streambox has violated provisions of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 et seq., by distributing and marketing products known as the Streambox VCR and the Ripper. RealNetworks also contends that another Streambox product, known as the Ferret, is unlawfully designed to permit consumers to make unauthorized modifications to a software program on which RealNetworks holds the copyright.

…

Finding of Fact

RealNetworks

…

2. RealNetworks offers products that enable consumers to access audio and video content over the Internet through a process known as "streaming." When an audio or video clip is "streamed" to a consumer, no trace of the clip is left on the consumer's computer, unless the content owner has permitted the consumer to download the file.

…

4. … To guard against the unauthorized copying and redistribution of their content, many copyright owners do not make their content available for downloading, and instead distribute the content using streaming technology in a manner that does not permit downloading.

…

RealNetworks' Products

…

10. To download streaming content distributed by a RealServer, … a consumer must employ a "RealPlayer." The RealPlayer is a software program that resides on an end-user's computer and must be used to access and play a streaming RealMedia file that is sent from a RealServer.

RealNetworks' Security Measures

11. RealNetworks' products can be used to enable owners of audio and video content to make their content available for consumers to listen to or view, while at the same time securing the content against unauthorized access or copying.

12. The first of these measures, called the "Secret Handshake" by RealNetworks, ensures that files hosted on a RealServer will only be sent to a RealPlayer. The Secret Handshake is an authentication sequence which only RealServers and RealPlayers know. By design, unless this authentication sequence takes place, the RealServer does not stream the content it holds.

Is the RealPlayer a trusted system? Is the RealServer? Is the Secret Handshake a technological measure that effectively controls access to content? The Copy Switch?

13. By ensuring that RealMedia files hosted on a RealServer are streamed only to RealPlayers, RealNetworks can ensure that a second security measure, which RealNetworks calls the "Copy Switch," is given effect. … If a content owner does not turn on the Copy Switch in a RealMedia file, the RealPlayer will not allow an end-user to make a copy of that file. The file will simply "evaporate" as the user listens to or watches it stream.

14. Through the use of the Secret Handshake and the Copy Switch, owners of audio and video content can prevent the unauthorized copying of their content if they so choose.

…

17. Copyright owners also use Real Networks' technology so that end-users can listen to, but not record, music that is on sale, either at a Web site or in retail stores. Other copyright owners enable users to listen to content on a "pay-per-play" basis that requires a payment for each time the end-user wants to hear the content. Without the security measures afforded by RealNetworks, these methods of distribution could not succeed. End-users could make and redistribute digital copies of any content available on the Internet, undermining the market for the copyrighted original.

18. RealNetworks' success as a company is due in significant part to the fact that it has offered copyright owners a successful means of protecting against unauthorized duplication and distribution of their digital works.

The RealPlayer Search Functionality

19. In addition to its content playing and content protection capabilities, the RealPlayer enables end-users to search the Internet for audio and video content. Currently, a company known as Snap! LLC supplies the search services available to end-users through the RealPlayer under a contract with RealNetworks.

…

21. … RealNetworks maintains that it has earned several million dollars from its contract with Snap.

Streambox

22. … The Streambox products at issue in this case are known as the Streambox VCR, the Ripper, and the Ferret.

Streambox VCR

Can you think of a use for the "VCR" other then circumvention of the Secret Handshake in order to access and make copies of content? Does it matter if such a use exists? Why or why not?

23. … [T]he only function relevant to this case is the portions of the [Streambox] VCR that allow it to access and copy RealMedia files located on RealServers.

24. In order to gain access to RealMedia content located on a RealServer, the VCR mimics a RealPlayer and circumvents the authentication procedure, or Secret Handshake, that a RealServer requires before it will stream content. In other words, the Streambox VCR is able to convince the RealServer ... that the VCR is, in fact, a RealPlayer.

25. … The VCR … allows the end-user to download RealMedia files even if the content owner has used the Copy Switch to prohibit end-users from downloading the files.

26. The only reason for the Streambox VCR to circumvent the Secret Handshake and interact with a RealServer is to allow an end-user to access and make copies of content that a copyright holder has placed on a RealServer in order to secure it against unauthorized copying. In this way, the Streambox VCR acts like a "black box" which descrambles cable or satellite broadcasts so that viewers can watch pay programming for free. … The Streambox VCR circumvents both the access control and copy protection measures.

…

29. Once an unauthorized, digital copy of a RealMedia file is created it can be redistributed to others at the touch of a button.

30. Streambox's marketing of the VCR notes that end-users can "download RealAudio and RealMedia files as easily as you would any other file, then reap the benefits of clean, unclogged streams straight from your hard drive" and that the product can be used by "savvy surfers who enjoy taking control of their favorite Internet music/video clips."

…

Streambox Ripper

32. Streambox also manufactures and distributes a product called the Streambox Ripper. The Ripper is a file conversion application that allows conversion (adaptation) of files from RealMedia format to other formats such as .WAV, .RMA, and MP3. The Ripper also permits conversion of files between each of these formats, i.e., .WAV to .WMA and .WAV to MP3.

33. The Ripper operates on files which are already resident on the hard disk of the user's computer. The Ripper permits users to convert files that they have already created or obtained (presumably through legitimate means) from one format to another.

34. Streambox has proferred evidence that one potential use of the Ripper would be to permit copyright owners to translate their content directly from the RealMedia format into other formats that they may wish to utilize for their own work. Streambox has provided examples of various content owner who need a way to convert their own RealMedia files into different formats, such as .WAV for editing, or .WMA to accommodate those users who wish to access the content with a Windows Media Player instead of a RealPlayer. In addition, content which is freely available, such as public domain material and material which users are invited and even encouraged to access and copy, may be converted by the Ripper into a different file format for listening at a location other than the user's computer.

Streambox Ferret

…

36. When a consumer installs the Ferret as a plug-in to the RealPlayer, the RealPlayer's graphical user interface is configured with an added button, which allows the user to switch between the Snap search engine and the Streambox search engine. The use of the Ferret may also result in replacement of the "Snap.Com" logo that appears on the RealPlayer's graphical user interface with a "Streambox" logo.

…

Conclusions of the Law

…

Parts of the VCR Are Likely to Violate Sections 1201(a)(2) and 1201(b)

7. Under the DMCA, the Secret Handshake that must take place between a RealServer and a RealPlayer before the RealServer will begin streaming content to an end-user appears to constitute a "technological measure" that "effectively controls access" to copyrighted works. See 17 U.S.C. § 1201(a)(3)(B) (measure "effectively controls access" if it "requires the application of information or a process or a treatment, with the authority of the copyright holder, to gain access to the work"). …

8. In conjunction with the Secret Handshake, the Copy Switch is a "technological measure" that effectively protects the right of a copyright owner to control the unauthorized copying of its work. See 17 U.S.C. § 1201(b)(2)(B) (measure "effectively protects" right of copyright holder if it "prevents, restricts or otherwise limits the exercise of a right of a copyright owner"); 17 U.S.C. § 106(a) (granting copyright holder exclusive right to make copies of its work). …

9. Under the DMCA, a product or part thereof "circumvents" protections afforded a technological measure by "avoiding bypassing, removing, deactivating or otherwise impairing" the operation of that technological measure. 17 U.S.C. §§ 1201(b)(2)(A), 1201(a)(2)(A). Under that definition, at least a part of the Streambox VCR circumvents the technological measures RealNetworks affords to copyright owners. …

10. Given the circumvention capabilities of the Streambox VCR, Streambox violates the DMCA if the product or a part thereof: (i) is primarily designed to serve this function; (ii) has only limited commercially significant purposes beyond the circumvention; or (iii) is marketed as a means of circumvention. 17 U.S.C. §§ 1201(a)(2)(A-C), 1201(b)(b)(A-C). These three tests are disjunctive. Id. A product that meets only one of the three independent bases for liability is still prohibited. Here, the VCR meets at least the first two.

What does it mean to say that "a part of the Streambox VCR" is designed to circumvent access controls? Can any tool that circumvents access controls - even if it is designed exclusively to serve other functions - survive the first prong of this disjunctive test under the court's construction?

11. The Streambox VCR meets the first test for liability under the DMCA because at least a part of the Streambox VCR is primarily, if not exclusively, designed to circumvent the access control and copy protection measures that RealNetworks affords to copyright owners. 17 U.S.C. §§ 1201(a)(2)(A), 1201(b)(c)(A).

12. The second basis for liability is met because portion of the VCR that circumvents the Secret Handshake so as to avoid the Copy Switch has no significant commercial purpose other than to enable users to access and record protected content. 17 U.S.C. § 1201(a)(2)(B), 1201(b)(d)(B). There does not appear to be any other commercial value that this capability affords.

13. Streambox's primary defense to Plaintiff's DMCA claims is that the VCR has legitimate uses. In particular, Streambox claims that the VCR allows consumers to make "fair use" copies of RealMedia files, notwithstanding the access control and copy protection measures that copyright owner may have placed on that file.

Notwithstanding the applicability of Sony, does 17 USC 1201(c)(1) support Streambox's fair use defense?

14. The portions of the VCR that circumvent the secret handshake and copy switch permit consumers to obtain and redistribute perfect digital copies of audio and video files that copyright owners have made clear they do not want copied. For this reason, Streambox's VCR is entitled to the same "fair use" protections the Supreme Court afforded to video cassette recorders used for "time-shifting" in Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984).

…

16. … [T]he Sony decision did not involve interpretation of the DMCA. Under the DMCA, product developers do not have the right to distribute products that circumvent technological measures that prevent consumers from gaining unauthorized access to or making unauthorized copies of works protected by the Copyright Act. Instead, Congress specifically prohibited the distribution of the tools by which such circumvention could be accomplished. …

…

18. Streambox also argues that the VCR does not violate the DMCA because the Copy Switch that it avoids does not "effectively protect" against the unauthorized copying of copyrighted works as required by § 1201(a)(3)(B). Streambox claims this "effective" protection is lacking because an enterprising end-user could potentially use other means to record streaming audio content as it is played by the end-user's computer speakers. This argument fails because the Copy Switch, in the ordinary course of its operation when it is on, restricts and limits the ability of people to make perfect digital copies of a copyrighted work. The Copy Switch therefore constitutes a technological measure that effectively protects a copyright owner's rights under section. 1201(a)(3)(B).

19. In addition, the argument ignores the fact that before the Copy Switch is even implicated, the Streambox VCR has already circumvented the Secret Handshake to gain access to a unauthorized RealMedia file. That alone is sufficient for liability under the DMCA. See 17 U.S.C. § 1201(i)(e).

…

22. As set forth above, the Streambox VCR falls within the prohibitions of sections 1201(a)(2) and 1201(b)(1). …

…

RealNetworks Has Not Demonstrated that It Is Reasonably Likely to Succeed on its DMCA Claim With Respect to the Ripper.

27. RealNetworks also alleges that Streambox's marketing and distribution of the Ripper violates section 1201(b) (but not section 1201(a)(2)) of the DMCA.

…

34. In light of Streambox's demonstration that the Ripper has legitimate and commercially significant uses, RealNetworks has not shown that it is likely to succeed on its DMCA claims with respect to the product.

…

RealNetworks Has Demonstrated that It Is Entitled to a Preliminary Injunction with Respect to the Ferret

36. Finally, RealNetworks claims that Streambox commits contributory and/or vicarious copyright infringement by distributing the Ferret product to the public. In order to prevail on such claims, RealNetworks must demonstrate that consumers who use the Ferret as a plug-in to the RealPlayer infringe RealNetworks' rights as a copyright owner. RealNetworks alleges that consumers who install the Ferret as a plug-in application to a RealPlayer create an unauthorized derivative of the RealPlayer, thus violating RealNetwork's rights under 17 U.S.C. § 106(2).

…

41. … [T]he Court concludes that RealNetworks has raised serious questions going to the merits of its claim. It is undisputed that consumers who install the Ferret as a plug-in application to the RealPlayer cause the graphical interface of the RealPlayer to be modified, arguably creating a derivative work under 17 U.S.C. § 106(2) without the copyright owner's authorization. In addition, RealNetworks has prof[f]erred evidence that end[-]users who install the Ferret are violating a license agreement with RealNetworks.

…

Conclusion

Consistent with the findings of fact and conclusions of law above, the Court hereby ORDERS that:

During the pendency of this action, Defendant Streambox, Inc. and its officers, agents, servants, employees and attorneys, and those persons in active concert and participation with Streambox, Inc. who receive actual notice of this Preliminary Injunction, are restrained and enjoined from manufacturing, importing, licensing, offering to the public, or offering for sale:

a) versions of the Streambox VCR or similar products that circumvent or attempt to circumvent RealNetworks' technological security measures, and from participating or assisting in any such activity;

b) versions of the Streambox Ferret or similar products that modify RealNetworks' RealPlayer program, including its interface, its source code, or its object code, and from participating or assisting in any such activity.

Plaintiff's motion for a preliminary injunction with respect to the Streambox Ripper is DENIED.

This Order shall be effective immediately, on the condition that RealNetworks continues to maintain security with the Clerk in the amount of $ 1,000,000 for the payment of such costs and damages as may be incurred by Streambox if it is found that Streambox was wrongfully enjoined by this Order.

The TRO entered by Judge Coughenour on December 23, 1999, and extended by the Court until 5:00 p.m. on January 18, 2000, is hereby VACATED by this Order.

Why doesn't RealNetworks allege here that the Ripper violates 1201(a)(2)? What does the product do? In what ways might it violate 1201(a)(2)?

Is a showing of legitimate, commercially significant uses sufficient to defeat a claim under 1201(a)(2)?

Had RealNetworks deployed technological controls to protect the source code for its RealPlayer, could it bring a claim under the DMCA with respect to Streambox's development of the Ferret? Could Streambox raise an exemption from liability as a defense?

Notes and Questions

1) The movie industry and the technology industry have collaborated to create OnlyOnce, a DVD that is unusable after being played once. OnlyOnce DVDs go on sale for 2 dollars each. Oversimplified, the way the technology works is that the DVDs have a coating on them that degenerates as the disc is viewed for the first time (rendering the disc inoperable). Suppose Play4Ever, Inc. starts selling a chemical that, when brushed on a disc, keeps its OnlyOnce coating from decaying. The chemical is difficult to make, but the recipe starts making the rounds on the Internet. Two weeks after the chemical is invented, a friend of yours emails you the recipe, which she found on the internet website FreeMovies.com.

Has Play4Ever violated the DMCA? Has FreeMovies.com? Your friend? In answering these questions, be sure to cite specific provisions. How would you measure damages?

2) Life-Time, Inc., stuffs copies of its popular "Lifetimes" magazine with CD-ROMs. The CD-ROMs contain a huge collection of celebrity photos and interviews. Readers who use the CDs in their computers find that they can sample – i.e., get access to – up to three such interviews, selecting from a list. After the user selects and views three interviews, the program offers an 800 number that, when called, allows the user to purchase twenty more such interviews with a credit card for $9.95. After payment is verified, the caller is given an "unlock" code that causes the program to disgorge the additional requested interviews. Jane Doe buys a copy of Lifetimes, uses the CD, and – thanks to her undergraduate work in computer science – is able to crack the CD's protection scheme and view all 2,000 interviews at her leisure without paying for a single one.

Does the DMCA appear to proscribe this behavior? Can you argue that Jane has not violated the DMCA? Is your answer any different if these interviews are accessed at a website, and not on Jane's personal computer? What if Jane simply guesses the "codeword" needed to unlock the content?

Should the law penalize Jane in any way for what she did? If not, how might the DMCA be interpreted or applied so as to avoid criminalizing this behavior? How might it be rewritten? If so, are there other, better ways to proscribe this type of behavior? If this type of behavior is not penalized, are producers of content less likely to make it available in forms that risk exposing more than they mean to?

D. Criminal Sanctions under the DMCA

With annual revenues of $1.2 billion and over 2,800 employees, Adobe is the second largest PC software company in the U.S. In an effort to create and then lead the market for software that enables the digital distribution of books, Adobe developed the Adobe Acrobat eBook Reader. The eBook Reader gives users a friendly interface with which to view the text and graphics of a book. Adobe's product overview explains:

> The free Adobe Acrobat eBook Reader enables you to read high-fidelity eBooks on your notebook or desktop computer - no special hardware is needed! Only this reader software displays eBooks with the pictures, graphics, and rich fonts you've come to expect from printed books. Combining a vivid, elegant reading experience with an intuitive interface, Acrobat eBook Reader gives you all that eBooks have to offer.

Adoption of the technology by users is only half of the puzzle for Adobe. Development of the market for digital book distribution software also requires adoption of the technology by book publishers. Where end users demand a "vivid, elegant reading experience," book publishers (extremely weary of making their books available digitally after witnessing the "Napsterization" of the music industry) demand robust copyright protection. To this end, Adobe's eBook Reader is designed as a trusted system, offering publishers a spectrum of copyright protection options when encoding their content. Adobe's FAQ (for readers, not publishers) explains:

> Can I print and copy my e-books?
>
> To protect copyrights, publishers establish their own guidelines for how much of their e-books can be printed or copied. This means that these permissions will differ from book to book. For example, some of the free books from the Adobe Bookstore have no restrictions

> on copying and printing. Or, a publisher might give users the ability to print several pages of a cookbook within a set period of time.

Founded in 1990 and headquartered in Moscow, ElcomSoft is a software company that – according to the company's website – "specializes in producing Windows productivity and utility applications for businesses and individuals." Among the many software products developed by ElcomSoft is the Advanced eBook Processor ("AEBPR"), which used to be available for download from their site. As explained by an Electronic Frontier Foundation ("EFF") FAQ:

> ElcomSoft's Advanced eBook Processor (AEBPR) allegedly removes the technological protection from eBooks that are in Adobe's eBook format and converts them into Adobe's Portable Document Format [("PDF")], so that people can use eBooks in more expanded ways than currently available under the Adobe eBook format. It also allows the eBooks to be read or processed by third-party software, not just Adobe's eBook Reader software. In effect, the AEBPR program removes the various restrictions (against copying, printing, text-to-speech processing, etc.) that publishers can enable or disable under Adobe's digital rights management system. The program is designed to work only with eBooks that have been lawfully purchased from sales outlets.

To put it more succinctly, the program enables users to: i) disable the copyright protection controls deployed by book publishers using Adobe's software and ii) repackage their digital books in a variety of common formats without copyright controls.

Dmitry Sklyarov is a 27-year-old programmer and cryptographer formerly employed by ElcomSoft who has been researching cryptanalysis in furtherance of a Ph.D. he hopes to earn from a Moscow University. He is allegedly responsible for much of ElcomSoft's AEBPR, most notably, the decryption algorithms it employs to circumvent Adobe's copyright protection controls.

In its first criminal prosecution under the DMCA, the Department of Justice ("D.O.J.") has indicted both ElcomSoft and Sklyarov for violations stemming from the development and marketing of ElcomSoft's AEBPR. (Adobe officers brought ElcomSoft's AEBPR to the attention of the FBI on June 26, 2001.) Sklyarov was most likely targeted largely because of his plans to enter the United States (making it easier for the D.O.J. to persuade a U.S. court to exert jurisdiction over him). The EFF tells the dramatic story as follows:

> [Sklyarov] was invited to give a presentation at the DEF CON conference in Las Vegas about the electronic security research work he has performed as part of his PhD research. His presentation concerned the weaknesses in Adobe's eBook technology software. Dmitry was arrested at his hotel in Las Vegas, on 16 July, [2001,] as he was leaving to return to Russia.

For the D.O.J.'s description of Sklyarov's arrest, and the events leading up to that arrest, read their July 17, 2001 press release. In its August 28, 2001 press release, the D.O.J. reported:

> The United States Attorney's Office for the Northern District of California announced that Elcom Ltd. (also known as Elcomsoft Co. Ltd.) and Dmitry Sklyarov, 27, both of Moscow, Russia, were indicted today by a federal grand jury in San Jose, California on five counts of copyright violations.
>
> The defendants were each indicted on one count of conspiracy to traffic in technology primarily designed to circumvent, and marketed for use in circumventing, technology that protects a right of a copyright owner, in violation of Title 18, United States Code, Section 371; two counts of trafficking in technology primarily designed to circumvent technology that protects a right of a copyright owner, in violation of Title 17, United States Code, Section 1201(b)(1)(A); and two counts of trafficking in technology marketed for use in circumventing technology that protects a right of a copyright owner, in violation of Title 17, United States Code, Section 1201(b)(1)(C).
>
> This is the first indictment under the Digital Millennium Copyright Act ("DMCA"), enacted by Congress in 1998.

Sklyarov's arrest prompted outcries of outrage from software developers, civil libertarians and all who generally oppose the DMCA (for ideological or "practical" reasons). See, for example, the EFF site dedicated to the controversy and FreeSklyarov.org. He faced a maximum fine of $2.25 million and up to 25 years imprisonment. Not surprisingly, the D.O.J. promptly reached an agreement with Sklyarov, under the terms of which they have agreed not to prosecute him personally if he assists in their (criminal) prosecution of ElcomSoft. The D.O.J., in its December 13, 2001 press release, describes the deal as follows:

> The United States Attorney's Office for the Northern District of California announced that Dmitry Sklyarov entered into an agreement this morning with the United States and admitted his conduct in a hearing before U.S. District Judge Whyte in San Jose Federal Court.
>
> Under the agreement, Mr. Sklyarov agreed to cooperate with the United States in its ongoing prosecution of Mr. Sklyarov's former employer, Elcomsoft Co., Ltd. Mr. Skylarov will be required to appear at trial and testify truthfully, and he will be deposed in the matter. For its part, the United States agreed to defer prosecution of Mr. Sklyarov until the conclusion of the case against Elcomsoft or for one year, whichever is longer. Mr. Sklyarov will be permitted to return to Russia in the meantime, but will be subject to the Court's supervision, including regularly reporting by telephone to the Pretrial Services Department. Mr. Sklyarov will be prohibited from violating any laws during the year, including copyright laws. The United States agreed that, if Mr. Sklyarov successfully completes the obligations in the agreement, it will dismiss the charges pending against him at the end of the year or when the case against Elcomsoft is complete.

ElcomSoft moved to dismiss the indictments on the grounds that (among others): i) the DMCA is in violation of ElcomSoft's Due Process rights (unconstitutionally vague and arbitrarily enforced) and ii) the DMCA is in violation of Elcomsoft's First Amendment rights. On May 8, 2002, Judge Whyte denied ElcomSoft's motion to dismiss the complaint on constitutional grounds.

The trial against ElcomSoft – the first criminal trial under the DMCA – began on August 26, 2002 before Judge Ronald Whyte of the U.S. District Court for the Northern District of California, as this casebook entered the final stages of publication. ElcomSoft faced a maximum fine of $2.5 million.

Notes and Questions

Is there any legitimate use for Elcomsoft's product? If such a use exists and, thanks to that and other factors, the software is not deemed illegal, what assurance does a publisher have that Adobe's protections will be useful? Is the existence of a legitimate use enough to put a given piece of software in the clear? If not, what else is required?

E. Free Speech and the DMCA

Declan McCullagh
A Constitutional Right to Decode?
8:00 a.m. May 31, 2001 PDT
http://www.wired.com/news/print/0,1294,44183,00.html

> WASHINGTON — To the movies studios trying to rid the Net of a DVD-descrambling program, the "DeCSS" utility is akin to terrorware that governments have a responsibility to prohibit.
>
> In a 40 KB brief filed late Wednesday, the studios say that just as federal law outlaws "gambling devices, trafficking in satellite theft devices, and trafficking in cable signal theft devices," Congress has the duty to enact laws preventing U.S. websites from distributing DeCSS.

But to the Electronic Frontier Foundation, which is representing the opposite side, DeCSS is more like "instructions for a photocopier, recipes, books about fixing cars, and videos on baby care" that are constitutionally protected by guarantees of free expression.

This battle of the briefs, done in response to an appeals court's recent request for more information, brings into sharp focus a question the courts have been trying to answer for much of the last decade: Is computer code speech?

If it is, then the formidable shield of the First Amendment would guard software from all but the most vigorous attempts by Congress to regulate it. If not, then it could be strictly regulated by the government in much the same way as food products or medical equipment are, or even outlawed entirely.

So far, the U.S. Supreme Court has not answered this question, and rulings from the federal appeals courts aren't that much help. But the answer appears likely to influence the future of online movie distribution and what rights users have to watch DVDs on Linux computers.

The Sixth Circuit Court of Appeals said last year in an encryption case that "because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."

In 1999, the Ninth Circuit Court of Appeals took a more modest approach in another case involving encryption regulation, saying that source code can be speech in some circumstances. Stressed the court: "We emphasize the narrowness of our First Amendment holding. We do not hold that all software is expressive. Much of it surely is not."

Both cases include discussions of source code, meaning a program written in a language like C, Perl, or BASIC that's intended to be read by humans. Because it's written by humans for humans, because it often includes comments and even jokes, and because it has to be translated into machine instructions before it's executed, courts have treated it differently than executable code.

But the current lawsuit before the Second Circuit Court of Appeals covers both the DeCSS source code and DeCSS.exe, a compiled Windows utility that allows users to descramble DVDs and copy them or play them on their Linux computer. That makes the fight harder for EFF, since no court has concluded that object code should be protected by the complete shield of the First Amendment.

During oral arguments on May 1, the three-judge panel appeared to be siding with copyright over free speech, but then took the unusual step a week later of sending both sides 11 questions to answer. The queries included "Does the dissemination of DeCSS have both speech and non-speech elements?" and "Does the use of DeCSS to decrypt an encrypted DVD have both speech and non-speech elements?"

EFF's 40 KB response was an unwavering affirmative. "DeCSS itself has no non-speech elements. It is a set of instructions written in a specific professional language that expresses ideas to those who can read that language," EFF said, saying that while DeCSS could be used to infringe copyrights, it has many non-infringing uses as well.

EFF, which is representing 2600 magazine, stressed that their client is a legitimate publication with First Amendment rights: The word "magazine" appears nine times in EFF's reply, but none in the response from the movie studios.

For their part, the studios see it as an open-and-shut case of copyright violation, saying the First Amendment does not protect the "right to distribute decryption devices that would enable every person in the nation (and millions more around the world) to make a complete, decrypted copy of pre-recorded DVDs, which would then be available for further copying or transmission over the Internet."

Their brief argues that neither the creation or distribution of DeCSS is related to free speech, and says the question of whether the use of DeCSS has any speech components is irrelevant: "The use of a copying machine to infringe a copyright might perhaps be said to have 'speech elements.'"

2600 is appealing its loss after a trial that took place last summer. U.S. District Judge Lewis Kaplan ruled last year that distributing the Windows utility violates the DMCA.

Kaplan largely sided with the studios, but did concede that "the distinction between source and object code is not as crystal clear as it first appears."

A decision from the Second Circuit could come at any time, and both sides have pledged to appeal a loss all the way to the Supreme Court.

DVD Copy Control Association v. Bunner

93 Cal. App. 4th 648, 60 U.S.P.Q.2D (BNA) 1803

Premo, Acting P.J.

This appeal arises from an action for injunctive relief brought under the Uniform Trade Secrets Act, Civil Code section 3426.1, et. seq. After learning that its trade secret had been revealed in DVD decryption software published on the Internet, plaintiff DVD Copy Control Association (DVDCCA) sought an injunction against defendant Andrew Bunner and numerous other Internet web-site operators to prevent future disclosure or use of the secret.

…

In October 1999, a computer program entitled "DeCSS" was posted on the Internet allegedly by Jon Johansen, a 15 year old resident of Norway. DeCSS consists of computer source code which describes a method for playing an encrypted DVD on a non-CSS-equipped DVD player or drive. Soon after its initial publication on the Internet, DeCSS appeared on numerous web sites throughout the world, including the web site of defendant Andrew Bunner. In addition, many individuals provided on their web sites "links" to copies of DeCSS on other web sites without republishing DeCSS themselves.

…

The first question we consider is whether DeCSS is "speech" that is within the scope of the First Amendment. The application of the First Amendment does not depend on whether the publication occurred on the Internet or by traditional means. (*Reno v. American Civil Liberties Union* (1997) 521 U.S. 844, 870, 117 S.Ct. 2329, 138 L.Ed.2d 874.) Likewise, it makes no difference that Bunner is a republisher rather than the original author of DeCSS. "It would be anomalous if the mere fact of publication and distribution were somehow deemed to constitute 'conduct' which in turn destroyed the right to freely publish." (*Wilson v. Superior Court, supra,* 13 Cal.3d at p. 660, 119 Cal.Rptr. 468, 532 P.2d 116.) "[A] naked prohibition against disclosures is fairly characterized as a regulation of pure speech." (*Bartnicki v. Vopper* (2001) 532 U.S. 514, ——, 121 S.Ct. 1753, 1761, 149 L.Ed.2d 787 (*Bartnicki*).) Nor does it matter that the disclosure was made by an individual on his web site rather than a media publication in a newspaper. The right to freedom of speech "does not restrict itself 'depend[ing] upon the identity' or legal character of the speaker, 'whether corporation, association, union, or individual.' " (*Gerawan Farming, Inc. v. Lyons* (2000) 24 Cal.4th 468, 485, 101 Cal.Rptr.2d 470, 12 P.3d 720; *Bartnicki v. Vopper, supra,* 532 U.S. at p. —— [121 S.Ct. at p. 1760], fn. 8.)

DVDCCA has not alleged that Bunner engaged in any expressive "conduct" by posting DeCSS on his web site. Nor is there any indication in the record that Bunner engaged in conduct mixed with speech. DVDCCA does suggest, however, that DeCSS is insufficiently expressive because it is composed of source code and has a functional aspect. "The issue of whether or not the First Amendment protects encryption source code is a difficult one because source code has both an expressive feature and a functional feature. The United States does not dispute that it is possible to use encryption source code to represent and convey information and ideas about cryptography and that encryption source code can be used by programmers and scholars for such informational purposes. Much like a mathematical or

> scientific formula, one can describe the function and design of encryption software by a prose explanation; however, for individuals fluent in a computer programming language, source code is the most efficient and precise means by which to communicate ideas about cryptography. [§] ... The fact that a medium of expression has a functional capacity should not preclude constitutional protection. [§] ... [§] ... [C]omputer source code, though unintelligible to many, is the preferred method of communication among computer programmers. [§] Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment." (*Junger v. Daley* (6th Cir.2000) 209 F.3d 481, 484-485.)
>
> Like the CSS decryption software, DeCSS is a writing composed of computer source code which describes an alternative method of decrypting CSS-encrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS. If the source code were "compiled" to create object code, we would agree that the resulting composition of zeroes and ones would not convey ideas. (See generally *Junger v. Daley, supra,* 209 F.3d at pp. 482-483.) That the source code is capable of such compilation, however, does not destroy the expressive nature of the source code itself. Thus, we conclude that the trial court's preliminary injunction barring Bunner from disclosing DeCSS can fairly be characterized as a prohibition of "pure" speech.

Gallery of DeCSS descramblers

Those seeking to guarantee the full ambit of First Amendment protections for computer code argue that software is undistinguishable from the myriad other forms of expression. In an effort to support this argument, some have repackaged the DeCSS source code in various "creative" forms, blurring the lines between code and expression. The "Gallery of CSS Descramblers," located at http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/ , is a website that highlights several examples of this creative presentation of source code. Among many other examples, the site showcases the "DeCSS T-Shirt" and the "DeCSS Song." The site's author(s) explains:

> If code that can be directly compiled and executed may be suppressed under the DMCA, … but a textual description of the same algorithm may not be suppressed, then where exactly should the line be drawn? This web site was created to explore this issue, and point out the absurdity of [the] position that source code can be legally differentiated from other forms of written expression.

F. The DMCA as the U.S. implementation of WIPO Treaties

Enacted in 1998, the DMCA represents the U.S.'s implementation of the World Intellectual Property Organization ("WIPO") Copyright Treaty, adopted by the Diplomatic Conference on Dec. 20, 1996, WIPO Doc. CRNR/DC/94 (Dec. 23, 1996) and the WIPO Performances and Phonograms Treaty, adopted by the Diplomatic Conference on Dec. 20, 1996, WIPO Doc. CRNR/DC/95 (Dec. 23, 1996).

Pamela Samuelson

Intellectual Property And The Digital Economy: Why The Anti-Circumvention Regulations Need To Be Revised

14 Berkeley Tech. L. J. 519 (1999)

Available at: http://www.sims.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm)

> The WIPO Copyright Treaty established several norms about applying copyright law in the digital environment. They include:

1) copyright owners should have an exclusive right to control the making of copies of their works in digital form,

2) copyright owners should have an exclusive right to control the communication of their works to the public,

3) countries can continue to apply existing exceptions and limitations, such as fair use, as appropriate in the digital environment, and can even create new exceptions and limitations appropriate to the digital environment,

4) merely providing facilities for the communication of works should not be a basis for infringement liability,

5) it should be illegal to tamper with copyright management information insofar as this would facilitate or conceal infringement in the digital environment, and

6) countries should have "adequate legal protection and effective legal remedies against the circumvention of effective technological measures" used by copyright owners to protect their works from infringing uses.

To the extent that uncertainties about how copyright law should apply in the digital environment were impeding the growth of a global market in electronic intellectual property products, there was reason to be optimistic that conclusion of this treaty would remove these blockages and allow e-commerce to flourish. These norms are as "predictable, minimalist, consistent, and simple" components of a legal environment for commerce as one could expect copyright professionals to devise. Thus, the WIPO treaty itself established norms compatible with … the needs of the digital economy. That nearly one hundred sixty nations signed this treaty indicated a strong consensus that digital works should be given appropriate protection on an international scale. This was very good news for U.S. digital economy industries.

The WIPO treaty digital copyright norms were, however, mostly old news for U.S. law. Its cases had already recognized the rights of authors to control digital reproductions of their works, as well as to control digital transmissions of their works to the public. Courts had invoked fair use in a number of digital copyright cases, and had refused to hold online service providers liable for infringing activities of users about which the providers had no knowledge. Because of the substantial accord between the WIPO treaty norms and existing U.S. law, the Clinton Administration initially considered whether the WIPO Copyright Treaty might even be sent to the Senate for ratification "clean" of implementing legislation. This would have avoided the kind of protracted legislative battle that occurred when Congress considered the Administration's White Paper legislation in 1996. Eventually, the Administration decided that implementing legislation was necessary for the U.S. to comply with the WIPO treaty provision requiring protection for the integrity of copyright management information. The DMCA implementation of this norm, which closely tracks the treaty language, was uncontroversial during the legislative process.

The U.S. could have asserted that its law already complied with the WIPO treaty's anti-circumvention norm. This norm was, after all, very general in character and provided treaty signatories with considerable latitude in implementation. Moreover, anti-circumvention legislation was new enough to many national intellectual property systems, and certainly to international law, to mean that there was no standard by which to judge how to instantiate the norm. The U.S. could have pointed to a number of statutes and judicial decisions that establish anti-circumvention norms. With U.S. copyright industries thriving in the current legal environment, it would have been fair to conclude that copyright owners already were adequately protected by the law. Even many of those who favor use of technical systems to protect digital copyrighted works have expressed skepticism about the need for or appropriateness of anti-circumvention regulations, at least at this stage. Let content producers build their technical fences, advised one prominent information economist, but do not legislatively reinforce those fences until experience proves the existence of one or more abuses in need of a

specific cure. However, the political reality and legislative dynamics of the WIPO Copyright Treaty implementation process were such that some sort of anti-circumvention provision appeared to be a necessary part of the bill.

Even if a reasoned assessment of U.S. law might have led policymakers to conclude that some additional anti-circumvention legislation was necessary or desirable, one would have thought that the Administration would have supported a "predictable, minimalist, consistent, and simple" legal rule, as its Framework principles call for. The Administration might have, for example, proposed to make it illegal to circumvent a technical protection system for purposes of engaging in or enabling copyright infringement. This, after all, was the danger that was said to give rise to the call for anti-circumvention regulations in the first place. Silicon Valley Representative Tom Campbell proposed such an approach in his alternative bill. If this same assessment caused policymakers to decide there was also a need for some regulation of circumvention technologies to promote electronic commerce, then a "predictable, minimalist, consistent, and simple" legal rule would have been to outlaw making or distributing a technology intentionally designed or produced to enable copyright infringement. Many "digital economy" firms and organizations supported the first of these proposals, and they would likely have supported the second if it had ever had a chance of being taken seriously.

Clinton Administration officials, bowing to the wishes of Hollywood and its allies, opted instead to support an unpredictable, overbroad, and maximalist set of anti-circumvention regulations. During Congressional consideration of these provisions, these regulations became complex and inconsistent for reasons that will become evident in later sections of this article. It was, in short, not the needs of the digital economy that drove adoption of the anti-circumvention provisions in the DMCA. Rather, what drove the debate was high rhetoric, exaggerated claims, and power politics from representatives of certain established but frightened copyright industries. These groups seem to believe they are so important to America that they should be allowed to control every facet of what Americans do with digital information. They also seem to think they are entitled to control the design and manufacture of all information technologies that can process digital information. The DMCA caters to their interests far more than to the interests of the innovative information technology sector or of the public.

Notes and Questions

Is the DMCA really "unpredictable, overbroad, and maximalist" in its implementation of the WIPO ideals it aims to codify? Do you think anti-circumvention legislation was necessary to bring U.S. copyright law in line with the WIPO treaties? Does the DMCA ultimately benefit consumers in guaranteeing that content will be made available in digital form?

Using Legislation to Mandate Creation and Compliance with Standards

So far we have examined the use of technology to restrict the capabilities of a mainstream personal computer – "trusted systems" – and the supporting legal controls that seek to limit outsiders' circumvention of those restrictions. These restrictions could come about as technology manufacturers and publishers come to agreement with each other and within their respective industries on standards. As we have seen, such agreement is not easy – there are many players, at times with quite divergent interests. In this section we review nascent attempts at gov-

ernment-mandated trusted systems as a way to rise above inter- and intra-industry barriers.

The attempts described in this section are quite sweeping -- to be effective they will have to apply to a broad range of computing devices. They represent a major departure from government policy to let technology develop as private markets demand. There exists one limited precedent, however, in American law with the Audio Home Recording Act of 1992. The AHRA was designed to settle a very specific problem: the impending release of digital audio tape foreshadowed an increase in piracy, since DATs could provide copies of compact discs without any degradation in quality from one generation to the next. The AHRA foreclosed this possibility by, in its essence, requiring DAT manufacturers to implement a form of content security for their products. DATs would have to distinguish between originals and copies, and for content self-labeled as restricted, the DATs would have to refuse to make a copy of a copy. The AHRA provides both a prelude and a bridge to the next round of legislation we discuss. It is the former because it shows a possible path of government-mandated technology standards; it is the latter because it was invoked by the recording industry against the first generation of portable MP3 players.

A. AHRA defines a trusted system

17 U.S.C. § 1002. Incorporation of copying controls

(a) Prohibition on importation, manufacture, and distribution. No person shall import, manufacture, or distribute any digital audio recording device or digital audio interface device that does not conform to—

(1) the Serial Copy Management System;

(2) a system that has the same functional characteristics as the Serial Copy Management System and requires that copyright and generation status information be accurately sent, received, and acted upon between devices using the system's method of serial copying regulation and devices using the Serial Copy Management System; or

(3) any other system certified by the Secretary of Commerce as prohibiting unauthorized serial copying.

(b) Development of verification procedure. The Secretary of Commerce shall establish a procedure to verify, upon the petition of an interested party, that a system meets the standards set forth in subsection (a)(2).

(c) Prohibition on circumvention of the system. No person shall import, manufacture, or distribute any device, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent any program or circuit which implements, in whole or in part, a system described in subsection (a).

Recording Industry Association of America v. Diamond Multimedia Systems Inc..

180 F.3d 1072 (9th Cir. 1999)

O'Scannlain, Circuit Judge:

In this case involving the intersection of computer technology, the Internet, and music listening, we must decide whether the Rio portable music player is a digital audio recording device subject to the restrictions of the Audio Home Recording Act of 1992.

I

This appeal arises from the efforts of the Recording Industry Association of America and the Alliance of Artists and Recording Companies (collectively, "RIAA") to enjoin the manufacture and distribution by Diamond Multimedia Systems ("Diamond") of the Rio portable

music player. The Rio is a small device (roughly the size of an audio cassette) with headphones that allows a user to download MP3 audio files from a computer and to listen to them elsewhere. …

A

…

Prior to the invention of devices like the Rio, [users of MP3 files, or compressed digital audio files,] had little option other than to listen to their downloaded digital audio files through headphones or speakers at their computers, playing them from their hard drives. The Rio renders these files portable. More precisely, once an audio file has been downloaded onto a computer hard drive from the Internet or some other source (such as a compact disc player or digital audio tape machine), separate computer software provided with the Rio (called "Rio Manager") allows the user further to download the file to the Rio itself via a parallel port cable that plugs the Rio into the computer. The Rio device is incapable of effecting such a transfer, and is incapable of receiving audio files from anything other than a personal computer equipped with Rio Manager.

… The Rio's sole output is an analog audio signal sent to the user via headphones. The Rio cannot make duplicates of any digital audio file it stores, nor can it transfer or upload such a file to a computer, to another device, or to the Internet. However, a flash memory card to which a digital audio file has been downloaded can be removed from one Rio and played back in another.

B

RIAA brought suit to enjoin the manufacture and distribution of the Rio, alleging that the Rio does not meet the requirements for digital audio recording devices under the Audio Home Recording Act of 1992, 17 U.S.C. § 1001 et seq. (the "Act"), because it does not employ a Serial Copyright Management System ("SCMS") that sends, receives, and acts upon information about the generation and copyright status of the files that it plays. See id. § 1002(a)(2). RIAA also sought payment of the royalties owed by Diamond as the manufacturer and distributor of a digital audio recording device. See id. § 1003.

The district court denied RIAA's motion for a preliminary injunction, holding that RIAA's likelihood of success on the merits was mixed and the balance of hardships did not tip in RIAA's favor. See generally Recording Indus. Ass'n of America, Inc. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624 (C.D. Cal. 1998) ("RIAA I"). RIAA brought this appeal.

II

The initial question presented is whether the Rio falls within the ambit of the Act. The Act does not broadly prohibit digital serial copying of copyright protected audio recordings. Instead, the Act places restrictions only upon a specific type of recording device. Most relevant here, the Act provides that "no person shall import, manufacture, or distribute any digital audio recording device . . . that does not conform to the Serial Copy Management System ["SCMS"] [or] a system that has the same functional characteristics." 17 U.S.C. § 1002(a)(1), (2) (emphasis added). The Act further provides that "no person shall import into and distribute, or manufacture and distribute, any digital audio recording device . . . unless such person records the notice specified by this section and subsequently deposits the statements of account and applicable royalty payments." Id. § 1003(a) (emphasis added). Thus, to fall within the SCMS and royalty requirements in question, the Rio must be a "digital audio recording device," which the Act defines through a set of nested definitions.

The Act defines a "digital audio recording device" as:

any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device, the digital recording function of which is designed or marketed for the primary purpose of, and that is capable of, making a digital audio copied recording for private use . . . .

Id. § 1001(3) (emphasis added).

A "digital audio copied recording" is defined as:

a reproduction in a digital recording format of a digital musical recording, whether that reproduction is made directly from another digital musical recording or indirectly from a transmission.

Id. § 1001(1) (emphasis added).

A "digital musical recording" is defined as:

a material object-

(i) in which are fixed, in a digital recording format, only sounds, and material, statements, or instructions incidental to those fixed sounds, if any, and

(ii) from which the sounds and material can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.

Id. § 1001(5)(A) (emphasis added).

In sum, to be a digital audio recording device, the Rio must be able to reproduce, either "directly" or "from a transmission," a "digital music recording."

III

We first consider whether the Rio is able directly to reproduce a digital music recording - which is a specific type of material object in which only sounds are fixed (or material and instructions incidental to those sounds). See id.

A

The typical computer hard drive from which a Rio directly records is, of course, a material object. However, hard drives ordinarily contain much more than "only sounds, and material, statements, or instructions incidental to those fixed sounds." Id. Indeed, almost all hard drives contain numerous programs (e.g., for word processing, scheduling appointments, etc.) and databases that are not incidental to any sound files that may be stored on the hard drive. Thus, the Rio appears not to make copies from digital music recordings, and thus would not be a digital audio recording device under the Act's basic definition unless it makes copies from transmissions.

Moreover, the Act expressly provides that the term "digital musical recording" does not include:

a material object-

(i) in which the fixed sounds consist entirely of spoken word recordings, or

(ii) in which one or more computer programs are fixed, except that a digital recording may contain statements or instructions constituting the fixed sounds and incidental material, and statements or instructions to be used directly or indirectly in order to bring about the perception, reproduction, or communication of the fixed sounds and incidental material.

Id. § 1001(5)(B) (emphasis added). As noted previously, a hard drive is a material object in which one or more programs are fixed; thus, a hard drive is excluded from the definition of digital music recordings. This provides confirmation that the Rio does not record "directly" from "digital music recordings," and therefore could not be a digital audio recording device unless it makes copies "from transmissions."

B

The district court rejected the exclusion of computer hard drives from the definition of digital music recordings under the statute's plain language (after noting its "superficial appeal") because it concluded that such exclusion "is ultimately unsupported by the legislative history, and contrary to the spirit and purpose of the [Act]." *RIAA I*, 29 F. Supp. 2d at 629. We need not resort to the legislative history because the statutory language is clear. *See City of Auburn v. United States*, 154 F.3d 1025, 1030 (9th Cir. 1998) ("Where statutory command is straightforward, 'there is no reason to resort to legislative history.'" (quoting *United States v. Gonzales*, 520 U.S. 1, 6, 137 L. Ed. 2d 132, 117 S. Ct. 1032 (1997))). Nevertheless, we will address the legislative history here, because it is consistent with the statute's plain meaning and because the parties have briefed it so extensively.

1

The Senate Report states that "if the material object contains computer programs or data bases that are not incidental to the fixed sounds, then the material object would not qualify" under the basic definition of a digital musical recording. S. Rep. 102-294 (1992), reprinted at 1992 WL 133198, at *118-19. The Senate Report further states that the definition "is intended to cover those objects commonly understood to embody sound recordings and their underlying works." Id. at *97. A footnote makes explicit that this definition only extends to the material objects in which songs are normally fixed: "that is recorded compact discs, digital audio tapes, audio cassettes, long-playing albums, digital compact cassettes, and minidiscs." Id. at n.36. There are simply no grounds in either the plain language of the definition or in the legislative history for interpreting the term "digital musical recording" to include songs fixed on computer hard drives.

RIAA contends that the legislative history reveals that the Rio does not fall within the specific exemption from the digital musical recording definition of "a material object in which one or more computer programs are fixed." 17 U.S.C. § 1001(5)(B)(ii). The House Report describes the exemption as "revisions reflecting exemptions for talking books and computer programs." H.R. Rep. 102-873(I) (1992), reprinted at 1992 WL 232935, at *35 (emphasis added); see also id. at *44 ("In addition to containing an express exclusion of computer programs in the definition of 'digital musical recording'. . . .") (emphasis added). We first note that limiting the exemption to computer programs is contrary to the plain meaning of the exemption. As Diamond points out, a computer program is not a material object, but rather, a literary work, see, e.g., Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1249 (3d Cir. 1983) ("[A] computer program . . . is a 'literary work.'"), that can be fixed in a variety of material objects, see 17 U.S.C. § 101 ("'Literary works' are works . . . expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books . . . tapes, disks, or cards, in which they are embodied.")

(emphasis added). Thus, the plain language of the exemption at issue does not exclude the copying of programs from coverage by the Act, but instead, excludes copying from various types of material objects. Those objects include hard drives, which indirectly achieve the desired result of excluding copying of programs. But by its plain language, the exemption is not limited to the copying of programs, and instead extends to any copying from a computer hard drive.

Moreover, RIAA's assertion that computer hard drives do not fall within the exemption is irrelevant because, regardless of that portion of the legislative history which addresses the exemption from the definition of digital music recording, see id. § 1001(5)(B)(ii), the Rio does not reproduce files from something that falls within the plain language of the basic definition of a digital music recording, see id. § 1001(5)(A).

2

The district court concluded that the exemption of hard drives from the definition of digital music recording, and the exemption of computers generally from the Act's ambit, "would effectively eviscerate the [Act]" because "any recording device could evade [ ] regulation simply by passing the music through a computer and ensuring that the MP3 file resided momentarily on the hard drive." RIAA I, 29 F. Supp. 2d at 630. While this may be true, the Act seems to have been expressly designed to create this loophole.

a

Under the plain meaning of the Act's definition of digital audio recording devices, computers (and their hard drives) are not digital audio recording devices because their "primary purpose" is not to make digital audio copied recordings. See 17 U.S.C. § 1001(3). Unlike digital audio tape machines, for example, whose primary purpose is to make digital audio copied recordings, the primary purpose of a computer is to run various programs and to record the data necessary to run those programs and perform various tasks. The legislative history is consistent with this interpretation of the Act's provisions, stating that "the typical personal computer would not fall within the definition of 'digital audio recording device,'" S. Rep. 102-294, at *122, because a personal computer's "recording function is designed and marketed primarily for the recording of data and computer programs," id. at *121. Another portion of the Senate Report states that "if the 'primary purpose' of the recording function is to make objects other than digital audio copied recordings, then the machine or device is not a 'digital audio recording device,' even if the machine or device is technically capable of making such recordings." Id. (emphasis added). The legislative history thus expressly recognizes that computers (and other devices) have recording functions capable of recording digital musical recordings, and thus implicate the home taping and piracy concerns to which the Act is responsive. Nonetheless, the legislative history is consistent with the Act's plain language - computers are not digital audio recording devices.

b

In turn, because computers are not digital audio recording devices, they are not required to comply with the SCMS requirement and thus need not send, receive, or act upon information regarding copyright and generation status. See 17 U.S.C. § 1002(a)(2). And, as the district court found, MP3 files generally do not even carry the codes providing information regarding copyright and generation status. See RIAA I, 29 F. Supp. 2d at 632. Thus, the Act seems designed to allow files to be "laundered" by passage through a computer, because even a device with SCMS would be able to download MP3 files lacking SCMS codes from a computer hard drive, for the simple reason that there would be no codes to prevent the copying.

Again, the legislative history is consistent with the Act's plain meaning. As the Technical Reference Document that describes the SCMS system explains, "digital audio signals . . . that have no information concerning copyright and/or generation status shall be recorded by the [digital audio recording] device so that the digital copy is copyright asserted and original generation status." Technical Reference Document for the Audio Home Recording Act of 1992, II-A, Par. 10, reprinted in H.R. Rep. 102-780(I), 32, 43 (1992) (emphasis added). Thus, the incorporation of SCMS into the Rio would allow the Rio to copy MP3 files lacking SCMS codes so long as it marked the copied files as "original generation status." And such a marking would allow another SCMS device to make unlimited further copies of such "original generation status" files, see, e.g., H.R. Rep. 102-873(I), at *47 ("Under SCMS . . . consumers will be able to make an unlimited number of copies from a digital musical recording."), despite the fact that the Rio does not permit such further copies to be made because it simply cannot download or transmit the files that it stores to any other device. Thus, the Rio without SCMS inherently allows less copying than SCMS permits.

c

In fact, the Rio's operation is entirely consistent with the Act's main purpose - the facilitation of personal use. As the Senate Report explains, "the purpose of [the Act] is to ensure the right of consumers to make analog or digital audio recordings of copyrighted music for their private, noncommercial use." S. Rep. 102-294, at *86 (emphasis added). The Act does so through its home taping exemption, see 17 U.S.C. § 1008, which "protects all noncommercial copying by consumers of digital and analog musical recordings," H.R. Rep. 102-873(I), at *59. The Rio merely makes copies in order to render portable, or "space-shift," those files that already reside on a user's hard drive. Cf. Sony Corp. of America v. Universal City Studios, 464 U.S. 417, 455, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984) (holding that "time-shifting" of copyrighted television shows with VCR's constitutes fair use under the Copyright Act, and thus is not an infringement). Such copying is paradigmatic noncommercial personal use entirely consistent with the purposes of the Act.

IV

Even though it cannot directly reproduce a digital music recording, the Rio would nevertheless be a digital audio recording device if it could reproduce a digital music recording "from a transmission." 17 U.S.C. § 1001(1).

A

The term "transmission" is not defined in Act, although the use of the term in the Act implies that a transmission is a communication to the public. See id. § 1002(e) (placing restrictions upon "any person who transmits or otherwise communicates to the public any sound recording in digital format") (emphasis added). In the context of copyright law (from which the term appears to have been taken), "to 'transmit' a performance or display is to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent." 17 U.S.C. § 101. The legislative history confirms that the copyright definition of "transmission" is sufficient for our purposes here. The Act originally (and circularly) provided that "[a] 'transmission' is any audio or audiovisual transmission, now known or later developed, whether by a broadcast station, cable system, multipoint distribution service, subscription service, direct broadcast satellite, or other form of analog or digital communication." S. Rep. 102-294, at *10. The Senate Report provides a radio broadcast as an example of a transmission. See id., at *119 (referring to "a transmission (e.g., a radio broadcast of a commercially released audio cassette)."). The parties do not really dispute the defi-

nition of transmission, but rather, whether indirect reproduction of a transmission of a digital music recording is covered by the Act.

B

RIAA asserts that indirect reproduction of a transmission is sufficient for the Rio to fall within the Act's ambit as a digital audio recording device. See 17 U.S.C. § 1001(1) (digital audio recording devices are those devices that are capable of making "a reproduction in a digital recording format of a digital musical recording, whether that reproduction is made directly from another digital musical recording or indirectly from a transmission") (emphasis added). Diamond asserts that the adverb "indirectly" modifies the recording of the underlying "digital music recording," rather than the recording "from the transmission." Diamond effectively asserts that the statute should be read as covering devices that are capable of making a reproduction of a digital musical recording, "whether that reproduction is made directly[,] from another digital musical recording[,] or indirectly[,] from a transmission."

While the Rio can only directly reproduce files from a computer hard drive via a cable linking the two devices (which is obviously not a transmission), the Rio can indirectly reproduce a transmission. For example, if a radio broadcast of a digital audio recording were recorded on a digital audio tape machine or compact disc recorder and then uploaded to a computer hard drive, the Rio could indirectly reproduce the transmission by downloading a copy from the hard drive. Thus, if indirect reproduction of a transmission falls within the statutory definition, the Rio would be a digital audio recording device.

1

RIAA's interpretation of the statutory language initially seems plausible, but closer analysis reveals that it is contrary to the statutory language and common sense. The focus of the statutory language seems to be on the two means of reproducing the underlying digital music recording - either directly from that recording, or indirectly, by reproducing the recording from a transmission. RIAA's interpretation of the Act's language (in which "indirectly" modifies copying "from a transmission," rather than the copying of the underlying digital music recording) would only cover the indirect recording of transmissions, and would omit restrictions on the direct recording of transmissions (e.g., recording songs from the radio) from the Act's ambit. This interpretation would significantly reduce the protection afforded by the Act to transmissions, and neither the statutory language nor structure provides any reason that the Act's protections should be so limited. Moreover, it makes little sense for the Act to restrict the indirect recording of transmissions, but to allow unrestricted direct recording of transmissions (e.g., to regulate second-hand recording of songs from the radio, but to allow unlimited direct recording of songs from the radio). Thus, the most logical reading of the Act extends protection to direct copying of digital music recordings, and to indirect copying of digital music recordings from transmissions of those recordings.

2

Because of the arguable ambiguity of this passage of the statute, recourse to the legislative history is necessary on this point. Cf. Moyle v. Director, Office of Workers' Compensation Programs, 147 F.3d 1116, 1120 (9th Cir. 1998) ("If the statute is ambiguous, [this court] consults the legislative history, to the extent that it is of value, to aid in [its] interpretation."), cert. denied, 143 L. Ed. 2d 541, 119 S. Ct. 1454 (1999). The Senate Report states that "a digital audio recording made from a commercially released compact disc or audio cassette, or from a radio broadcast of a commercially released compact disc or audio cassette, would be a 'digital audio copied recording.'" S. Rep. 102-294, at *119 (emphasis added). This

statement indicates that the recording of a transmission need not be indirect to fall within the scope of the Act's restrictions, and thus refutes RIAA's proposed interpretation of the relevant language. Moreover, the statement tracks the statutory definition by providing an example of direct copying of a digital music recording from that recording, and an example of indirect copying of a digital music recording from a transmission of that recording. Thus the legislative history confirms the most logical reading of the statute, which we adopt: "indirectly" modifies the verb "is made" - in other words, modifies the making of the reproduction of the underlying digital music recording. Thus, a device falls within the Act's provisions if it can indirectly copy a digital music recording by making a copy from a transmission of that recording. Because the Rio cannot make copies from transmissions, but instead, can only make copies from a computer hard drive, it is not a digital audio recording device.

Would an mp3 player that had an infrared port, capable of beaming copies of its mp3 files to other such players, be covered by the AHRA? How about one that was simply a portable hard drive – capable of shifting files of any kind, including mp3s, back and forth between different computers, while also being able to play its mp3 files through a set of headphones?

V

For the foregoing reasons, the Rio is not a digital audio recording device subject to the restrictions of the Audio Home Recording Act of 1992. The district court properly denied the motion for a preliminary injunction against the Rio's manufacture and distribution. Having so determined, we need not consider whether the balance of hardships or the possibility of irreparable harm supports injunctive relief.

AFFIRMED.

Note: The Resonance between the AHRA and CSS

Earlier in this chapter, we considered the controversy over DeCSS. In exploring the significance of this dispute, we noted the role of the CSS technology in forcing DVD player manufacturers to submit to the private law of CSS technology licenses as granted by the DVDCCA, a trade association of businesses in the motion picture industry.

The AHRA is public law that mandates compliance with certain copyright protection controls and exerts royalties for the music industry from manufacturers of digital audio recording devices. It is the result of an extensive lobbying effort on the part of the trade associations representing the music industry.

Both the AHRA and the CSS technology (and its licensing terms), then, serve to empower the holders of copyrights to exert control over the manufacturers of devices that deliver their content.

The development of CSS technology and the associated terms for licensing the technology can be seen as a more direct, fully private means of controlling hardware manufacturers. Assuming the technology is sound, the terms of the licenses for CSS are as unavoidable for manufacturers as is the U.S. law embodied in the AHRA. (We leave it to the reader to consider the relative differences of privately controlled contract terms versus federal law and, similarly, remedies available for contract breach versus those which enforce public law.) The DMCA serves to deliver the "best of both worlds." Private technological efforts (aimed at protecting copyright interests) are given the weight of public law. Private controls force compliance with private contract. Efforts to circumvent these controls contravenes public law. In effect, the DMCA empowers copyright holders to develop, in software, AHRA-like controls that have the full force of U.S. law behind them.

B. The Consumer Broadband and Digital Television Promotion Act

Judge O'Scannlain's opinion for the Ninth Circuit in *Recording Industry Association of America v. Diamond Multimedia Systems* is most significant for its holding that personal computers are not covered under the AHRA and computer manufacturers are, thus, not required to incorporate the copy control systems mandated by the AHRA (nor are computer manufacturers required to pay the royalties mandated by the AHRA).

In March of 2002, Senator Hollings (D-SC) introduced the "Consumer Broadband and Digital Television Promotion Act" ("CBDTPA"). Formerly known as the "Systems Standards and Certification Act," or "SSSCA," the proposed legislation would prohibit the sale or distribution of nearly any kind of electronic device – includ-

ing, most notably, personal computers – unless the device complies with copy-protection standards to be set by the federal government. The copy-protection standards envisioned would mandate the incorporation of what is effectively a trusted system architecture, specifying security and interoperability requirements.

In effect, the CBDTPA would be the "next generation AHRA"; it would cover all forms of media – not just audio – and all forms of devices. A diverse, powerful body of intellectual property interests (including, for example, the music recording and film industries) heralds the CBDTPA as an overdue, fundamentally necessary measure. Absent legislation to overcome the "weakest link" problem, viz. digital media is only as secure as the weakest level of security embodied by all of the devices on which it can be accessed, they argue that intellectual property rights in digital assets can never be protected.

For the most part, academics and technology entrepreneurs oppose the bill vehemently. Among other complaints, they argue that the procedure set forth for developing the actual technology specifications affords the content and media industries undue influence in the ultimate legislation (the FCC would have one year to consider a compromised proposal to be submitted by "digital media device manufacturers, consumer groups and copyright owners"). They also take issue with the extremely broad definition of "digital media devices" contained in the bill (Senator Hollings himself has said, "any device that can legitimately play, copy or electronically transmit one or more categories of media also can be misused for illegal copyright infringement, unless special protection technologies are incorporated"). Lastly, they cite the risk that these technologies can be "abused" to afford content providers protections not guaranteed by law.

Most observers agree that the bill is unlikely to pass in its current form, though not as a result of opposition based on ideology. Many close to the issue think that the effort faces a greater likelihood of overall success if the industries touched by the legislation have more time to prepare and provide input before legislation is passed. This timing consideration is most likely the one that would have greatest weight in defeating the bill. Indeed, if the legislators' own statements during committee hearings about the bill are to be credited, the introduction rather than actual passage of the legislation is itself meant to be a spur to the industry.

The CBDTPA is perhaps a useful bellwether of future legislation in this area. We reproduce it here to help give a sense of how a government might seek to actually develop industry-wide standards – including the level of specificity with which those standards would be couched.

Consumer Broadband and Digital Television Promotion Act

107th Congress, 2D Session, S. 2048

CONSUMER BROADBAND AND DIGITAL TELEVISION PROMOTION ACT

107TH CONGRESS, 2D SESSION, S. 2048

IN THE SENATE OF THE UNITED STATES

MARCH 21, 2002

Mr. HOLLINGS (for himself, Mr. STEVENS, Mr. INOUYE, Mr. BREAUX, Mr. NELSON of Florida, and Mrs. FEINSTEIN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

…

SEC. 2. FINDINGS.

The Congress finds the following:

(1) The lack of high quality digital content continues to hinder consumer adoption of broadband Internet service and digital television products.

(2) Owners of digital programming and content are increasingly reluctant to transmit their products unless digital media devices incorporate technologies that recognize and respond to content security measures designed to prevent theft.

(3) Because digital content can be copied quickly, easily, and without degradation, digital programmers and content owners face an exponentially increasing piracy threat in a digital age.

(4) Current agreements reached in the marketplace to include security technologies in certain digital media devices fail to provide a secure digital environment because those agreements do not prevent the continued use and manufacture of digital media devices that fail to incorporate such security technologies.

(5) Other existing digital rights management schemes represent proprietary, partial solutions that limit, rather than promote, consumers' access to the greatest variety of digital content possible.

(6) Technological solutions can be developed to protect digital content on digital broadcast television and over the Internet.

(7) Competing business interests have frustrated agreement on the deployment of existing technology in digital media devices to protect digital content on the Internet or on digital broadcast television.

(8) The secure protection of digital content is a necessary precondition to the dissemination, and on-line availability, of high quality digital content, which will benefit consumers and lead to the rapid growth of broadband networks.

(9) The secure protection of digital content is a necessary precondition to facilitating and hastening the transition to high-definition television, which will benefit consumers.

(10) Today, cable and satellite have a competitive advantage over digital television because the closed nature of cable and satellite systems permit encryption, which provides some protection for digital content.

(11) Over-the-air broadcasts of digital television are not encrypted for public policy reasons and thus lack those protections afforded to programming delivered via cable or satellite.

(12) A solution to this problem is technologically feasible but will require government action, including a mandate to ensure its swift and ubiquitous adoption.

(13) Consumers receive content such as video or programming in analog form.

(14) When protected digital content is converted to analog for consumers, it is no longer protected and is subject to conversion into unprotected digital form that can in turn be copied or redistributed illegally.

(15) A solution to this problem is technologically feasible but will require government action, including a mandate to ensure its swift and ubiquitous adoption.

(16) Unprotected digital content on the Internet is subject to significant piracy, through illegal file sharing, downloading, and redistribution over the Internet.

(17) Millions of Americans are currently downloading television programs, movies, and music on the Internet and by using "file-sharing" technology. Much of this activity is illegal, but demonstrates consumers' desire to access digital content.

(18) This piracy poses a substantial economic threat to America's content industries.

(19) A solution to this problem is technologically feasible but will require government action, including a mandate to ensure its swift and ubiquitous adoption.

(20) Providing a secure, protected environment for digital content should be accompanied by a preservation of legitimate consumer expectations regarding use of digital content in the home.

(21) Secure technological protections should enable content owners to disseminate digital content over the Internet without frustrating consumers' legitimate expectations to use that content in a legal manner.

(22) Technologies used to protect digital content should facilitate legitimate home use of digital content.

(23) Technologies used to protect digital content should facilitate individuals' ability to engage in legitimate use of digital content for educational or research purposes.

SEC. 3. ADOPTION OF SECURITY SYSTEM STANDARDS AND ENCODING RULES.

(a) PRIVATE SECTOR EFFORTS.—

(1) IN GENERAL.—The Federal Communications Commission, in consultation with the Register of Copyrights, shall make a determination, not more than 12 months after the date of enactment of this Act, as to whether—

(A) representatives of digital media device manufacturers, consumer groups, and copyright owners have reached agreement on security system standards for use in digital media devices and encoding rules; and

(B) the standards and encoding rules conform to the requirements of subsections (d) and (e).

…

(b) AFFIRMATIVE DETERMINATION.—If the Commission makes a determination under subsection (a)(1) that an agreement on security system standards and encoding rules that conform to the requirements of subsections (d) and (e) has been reached, then the Commission shall—

(1) initiate a rulemaking, within 30 days after the date on which the determination is made, to adopt those standards and encoding rules; and

(2) publish a final rule pursuant to that rulemaking, not later than 180 days after initiating the rulemaking, that will take effect 1 year after its publication.

(c) NEGATIVE DETERMINATION.—If the Commission makes a determination under subsection (a)(1) that an agreement on security system standards and encoding rules that conform to the requirements of subsections (d) and (e) has not been reached, then the Commission—

(1) in consultation with representatives described in subsection (a)(1)(A) and the Register of Copyrights, shall initiate a rulemaking, within 30 days after the date on which the determination is made, to adopt security system standards and encoding rules that conform to the requirements of subsections (d) and (e); and

(2) shall publish a final rule pursuant to that rulemaking, not later than 1 year after initiating the rulemaking, that will take effect 1 year after its publication.

(d) SECURITY SYSTEM STANDARDS.—In achieving the goals of setting open security system standards that will provide effective security for copyrighted works, the security system standards shall ensure, to the extent practicable, that—

(1) the standard security technologies are—

(A) reliable;
(B) renewable;
(C) resistant to attack;
(D) readily implemented;
(E) modular;
(F) applicable to multiple technology platforms;
(G) extensible;
(H) upgradable;
(I) not cost prohibitive; and

Are these requirements well-defined and exhaustive? Can you think of additional requirements that should be included?

(2) any software portion of such standards is based on open source code.

(e) ENCODING RULES.—

(1) LIMITATIONS ON THE EXCLUSIVE RIGHTS OF COPYRIGHT OWNERS.—In achieving the goal of promoting as many lawful uses of copyrighted works as possible, while preventing as much infringement as possible, the encoding rules shall take into account the limitations on the exclusive rights of copyright owners, including the fair use doctrine.

What, exactly, are the requirements imposed with respect to the fair use exception to copyright? Could you build fair use into a complying system? How would the system know when to allow a use as "fair"?

(2) PERSONAL USE COPIES.—No person may apply a security measure that uses a standard security technology to prevent a lawful recipient from making a personal copy for lawful use in the home of programming at the time it is lawfully performed, on an over-the-air broadcast, premium or non-premium cable channel, or premium or non-premium satellite channel, by a television broadcast station (as defined in section 122(j)(5)(A) of title 17, United States Code), a cable system (as defined in section 111(f) of such title), or a satellite carrier (as defined in section 119(d)(6) of such title).

(f) MEANS OF IMPLEMENTING STANDARDS.—The security system standards adopted under subsection (b), (c), or (g) shall provide for secure technical means of implementing directions of copyright owners for copyrighted works.

Under the proposed CBDTPA, who formulates the standards? Can these standards be changed? By whom and under what conditions?

(g) COMMISSION MAY REVISE STANDARDS AND RULES THROUGH RULEMAKING.—

(1) IN GENERAL.—The Commission may conduct subsequent rulemakings to modify any security system standards or encoding rules established under subsection (b) or (c) or to adopt new security system standards that conform to the requirements of subsections (d) and (e).

…

(h) MODIFICATION OF TECHNOLOGY BY PRIVATE SECTOR.—

(1) IN GENERAL.—After security system standards have been established under subsection (b), (c), or (g) of this section, representatives of digital media device manufacturers, consumer groups, and copyright owners described in subsection (a)(1)(A) may modify the standard security technology that adheres to the security system standards rules established under this section if those representatives determine that a change in the technology is necessary because—

(A) the technology in use has been compromised; or

(B) technological improvements warrant upgrading the technology in use.

(2) IMPLEMENTATION NOTIFICATION.—The representatives described in paragraph (1) shall notify the Commission of any such modification before it is implemented or, if immediate implementation is determined by the representatives to be necessary, as soon thereafter as possible.

(3) COMPLIANCE WITH SUBSECTION (d) REQUIREMENTS.—The Commission shall ensure that any modification of standard security technology under this subsection conforms to the requirements of subsection (d).

SEC. 4. PRESERVATION OF THE INTEGRITY OF SECURITY.

An interactive computer service shall store and transmit with integrity any security measure associated with standard security technologies that is used in connection with copyrighted material such service transmits or stores.

SEC. 5. PROHIBITION ON SHIPMENT IN INTERSTATE COMMERCE OF NONCONFORMING DIGITAL MEDIA DEVICES.

(a) IN GENERAL.—A manufacturer, importer, or seller of digital media devices may not—

(1) sell, or offer for sale, in interstate commerce, or
(2) cause to be transported in, or in a manner affecting, interstate commerce,

a digital media device unless the device includes and utilizes standard security technologies that adhere to the security system standards adopted under section 3.

(b) EXCEPTION.—Subsection (a) does not apply to the sale, offer for sale, or transportation of a digital media device that was legally manufactured or imported, and sold to the consumer, prior to the effective date of regulations adopted under section 3 and not subsequently modified in violation of section 6(a).

SEC. 6. PROHIBITION ON REMOVAL OR ALTERATION OF SECURITY TECHNOLOGY; VIOLATION OF ENCODING RULES.

(a) REMOVAL OR ALTERATION OF SECURITY TECHNOLOGY.—No person may—

(1) knowingly remove or alter any standard security technology in a digital media device lawfully transported in interstate commerce; or

(2) knowingly transmit or make available to the public any copyrighted material where the security measure associated with a standard security technology has been removed or altered, without the authority of the copyright owner.

(b) COMPLIANCE WITH ENCODING RULES.—No person may knowingly apply to a copyrighted work, that has been distributed to the public, a security measure that uses a standard security technology in violation of the encoding rules adopted under section 3.

SEC. 7. ENFORCEMENT.

(a) IN GENERAL.—The provisions of section 1203 and 1204 of title 17, United States Code, shall apply to any violation of this Act as if—

(1) a violation of section 5 or 6(a)(1) of this Act were a violation of section 1201 of title 17, United States Code; and

(2) a violation of section 4 or section 6(a)(2) of this Act were a violation of section 1202 of that title.

(b) STATUTORY DAMAGES.—A court may award damages for each violation of section 6(b) of not less than $200 and not more than $2,500, as the court considers just.

…

SEC. 9. DEFINITIONS.

In this Act:

(1) STANDARD SECURITY TECHNOLOGY.—The term "standard security technology" means a security technology that adheres to the security system standards adopted under section 3.

(2) INTERACTIVE COMPUTER SERVICE.—The term "interactive computer service" has the meaning given that term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(3) DIGITAL MEDIA DEVICE.—The term "digital media device" means any hardware or software that—

(A) reproduces copyrighted works in digital form;

(B) converts copyrighted works in digital form into a form whereby the images and sounds are visible or audible; or

(C) retrieves or accesses copyrighted works in digital form and transfers or makes available for transfer such works to hardware or software described in subparagraph (B).

(4) COMMISSION.—The term "Commission" means the Federal Communications Commission.

Questions

Can you envision a broad range of systems that could be produced in compliance with these standards or a narrow one?

Coda

Is it better for private industry rather than the government to generate standards for content protection? If private industry, would consumer preferences/freedoms be represented solely by consumers' roles as drivers of the market for new products and the content they convey? Can standards come about in the absence of a mandate?

What changes, if any, ought to be made to the CBDTPA? How much of the actual standards development is left to private industry?

Is the CBDTPA the beginning of the end of open networks?