



Confronting Digital Piracy

*Intellectual Property Protection
in the Internet Era*

by Shane Ham and Robert D. Atkinson

About the Technology and New Economy Project

The Project's mission is to educate federal, state, and local policymakers about what drives the New Economy, and to promote policies that encourage technological advances, economic innovation, and entrepreneurship. Among the key principles guiding the Project's work are the following:

- ▶ Higher productivity and faster economic growth are prerequisites for expanding opportunity and raising living standards.
- ▶ The key factors driving economic growth are science and technology, world-class education and skills, organizational innovation, robust competition, and open global trade.
- ▶ Markets are the best drivers of growth and innovation, but public action can and should create conditions in which innovation can flourish. This requires updating public fiscal, investment, and regulatory policies at every level.
- ▶ Archaic regulatory barriers to competition and innovation should be replaced with "open architecture" principles that do not favor one technology, industry, or profession over another.
- ▶ Government should be reinvented to be as fast, responsive, and flexible as the economy and society with which it interacts. The new model of governing is decentralized, non-bureaucratic, catalytic, and empowering.
- ▶ We should take active steps to extend the benefits of technology and innovation to all citizens, reversing past trends toward economic inequality.

The goals of the Technology and New Economy Project are a natural extension of the mission of the Progressive Policy Institute, which is to define and promote a new progressive politics for America in the 21st century. The Institute's core philosophy rises from the belief that America is ill-served by an obsolete left-right debate that is out of step with the powerful forces reshaping our society and economy. The Institute believes in adapting the progressive tradition in American politics to the realities of the Information Age by advocating a "Third Way" approach, beyond the liberal impulse to defend the bureaucratic status quo and the conservative bid to dismantle government.

The Progressive Policy Institute is a project of the Third Way Foundation. Will Marshall is president of the Institute. Al From is chairman of the Third Way Foundation. For further information, to view this report online, or to order other PPI publications, please call, write, or visit the PPI website:

600 Pennsylvania Avenue, SE, Suite 400
Washington, DC 20003
www.ppionline.org
Email: *ppiinfo@dlcppi.org*
Phone: (202) 546-0007 Fax: (202) 544-5014

Contents

Introduction	2
The Problem of Piracy in the Digital Era	5
<i>Why is Threat of Piracy Greater Today?</i>	5
<i>How Can Content Be Stolen?</i>	7
<i>What Are Legitimate Uses of Copying Content?</i>	8
Meeting in the Middle: Encouraging Purchasing Over Piracy	10
<i>Making Illegal Copying More Difficult</i>	10
<i>Policy Recommendations for Making Illegal Copying More Difficult</i>	14
<i>Making Purchasing of Content Easier</i>	15
<i>Policy Recommendations for Making Purchasing of Content Easier</i>	17
Conclusion	19
Endnotes	20

Confronting Digital Piracy: Intellectual Property Protection in the Internet Era

Of all the industries that have been revolutionized by the rise of digital technology and the global Internet, few have been hit as hard as the “content” industries—the producers of music, movies, television programs, interactive software, books, photos, and periodicals. The Internet has made global distribution of content easier than ever, with the ultimate promise of slashing costs by reducing the role of middlemen who produce, distribute, and sell the physical copies. Unfortunately, the digital era also has a serious downside for content producers: It has made it easier than ever for consumers to get access to content without paying for it.

There is no doubt that digital copying and transmission of intellectual property is poised to do major damage to the content industries. The recording industry has been hardest hit thus far, because digital song files are small enough to transmit quickly: Global sales of music fell 8 percent in 2002 alone, due in part to online piracy.¹ The peer-to-peer networks that allow individuals to download pirated material anonymously cover every conceivable kind of content: films, television programs, software, even the latest Harry Potter novel.² The vexing part of the problem is that this piracy is not a massive criminal conspiracy, but rather the collective actions of millions of otherwise law-abiding Internet users of all ages who have grown accustomed to the culture of free content that is the hallmark of the Internet. Many people have a hard time distinguishing between the vast amount of music, video games, and other content available legitimately for free and the illegal pirated content.

This is not merely a battle between giant media conglomerates and a group of cyberlibertarians who want to rethink copyright law. Widespread piracy over the Internet seriously harms the artists, both the famous and struggling, who create content, as well as the technicians—sound engineers, editors, set designers, game programmers—who produce it.

In the music industry, artists ranging from Eminem to Luciano Pavarotti have joined forces to protect their livelihood against the new digital threat. As the popular band Barenaked Ladies points out, “When the Gap went online, T-shirts didn’t become free.”³

This rampant piracy has serious economic implications reaching far beyond the lost revenue of the stealing itself. Many content providers have resisted embracing digital distribution and online business models in part because of fear that digital piracy will eventually destroy their businesses—as they say, it is impossible to compete with free. But is that really so? The degree to which that assumption is true will form the basis of many public policy decisions.

Of course, virtually every product sold to consumers is vulnerable to theft, which is why retail stores spend money to prevent shoplifting. Content is particularly vulnerable in the digital environment, however, because an infinite number of perfect copies can be made from just one original and because those copies can be distributed cheaply around the globe using the Internet. Completely eliminating this kind of piracy is impossible. Once one copy of a song or film is created free of copy protection measures, it can multiply like a virus until it is widely available. Until now, this has been a problem confined mostly to the music and software industries, but with the growth of high-speed Internet connections, virtually every content industry is affected.

At the same time, if the content industries are not able to achieve some degree of protection for their intellectual property, there are two likely scenarios. One is a marked decrease in the production of high-quality content (along with the attendant trade and employment implications).⁴ The other possibility is a tighter lockdown of content through encryption and other technologies that greatly restrict consumer uses of content (along with the implications for consumers, device manufacturers, web portals, and other industries). Reaching an acceptable

level of protection, of course, will have costs and inconveniences; the goal should be to place those burdens, to the greatest extent possible, on the pirates themselves rather than on the content or technology industries or law-abiding consumers as a whole.

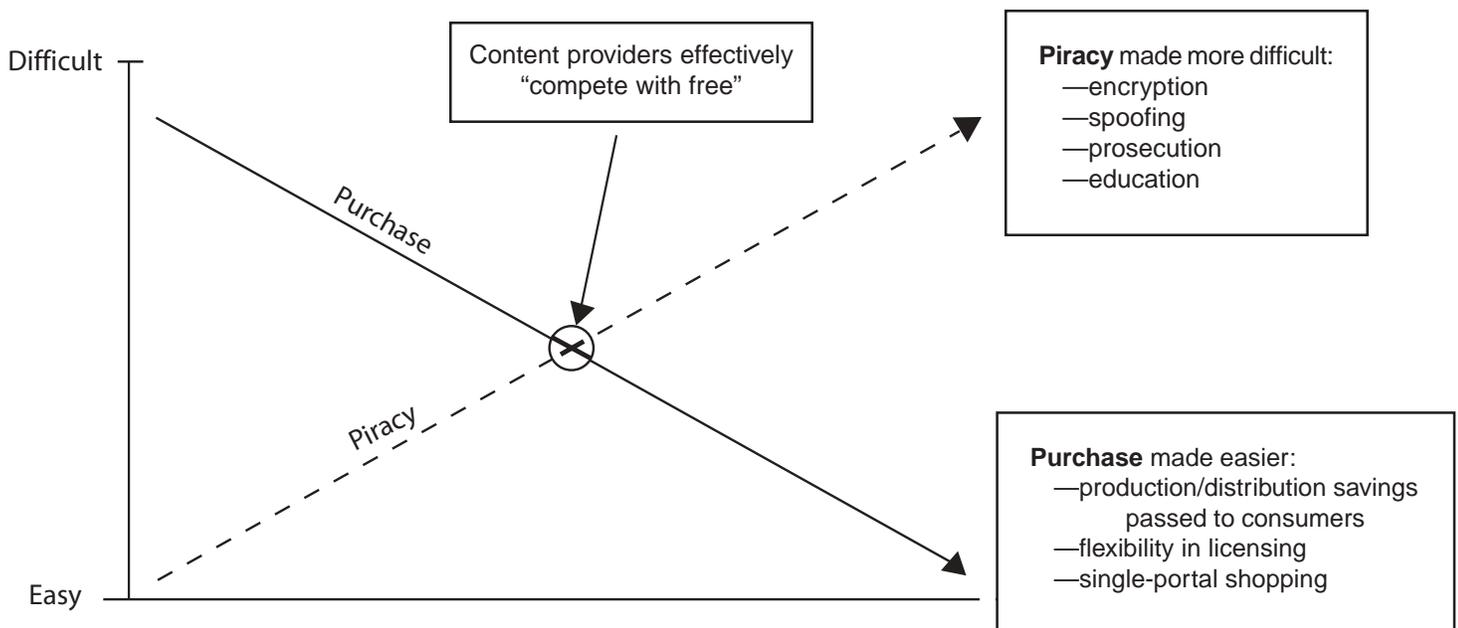
We believe it is possible, however, to keep piracy to a low and manageable level if two things happen. First, the inconvenience of piracy must increase, including the difficulty in finding and downloading pirated content, and the risk of getting caught and punished for doing so. Second, both public and private measures must be taken to make it easier for consumers to acquire content legally, by paying for the content that they download. The recent stunning success of the iTunes service,⁵ which sold over one million songs in its first week of operation alone, proves that consumers are willing to pay for content if it is easy to find, flexible to use, and reasonably priced. (Prices are poised to fall even more since printing and distribution of physical media can account for one-half the price consumers pay—costs that can be eliminated with digital distribution.)

This report argues that if content piracy is made more difficult and content purchasing is made easier, content providers will be able to maintain viable business models even when competing with illegal free downloads on peer-to-peer networks.

Pursuing a public policy agenda that facilitates these two changes will have immense economic impacts as content providers stop resisting the digital revolution and embrace the Internet to sell music, movies, software, and other content directly to consumers. This will move us toward the ultimate goal: an environment in which digitally transmitted content is widely available and the creators of the content are fairly compensated for their efforts. To reach this goal PPI recommends that:

- ▶ **Congress should give industry time to develop standards for protecting digital content.** Rather than rushing to impose deadlines for solving the piracy problems (or worse, creating government standards for copyright protection), the industry groups at work on the problem should be given an opportunity to complete the task under the watchful eye of Congress;
- ▶ **Once standards are developed, Congress should, if need be, mandate their implementation.** A legal requirement to comply with copy protection systems will eliminate the incentive to create “piracy-enabled” machines to compete with the computers, digital recorders, and other devices that conform with the industry-set standards;

Chart 1: Competing with Free



Confronting Digital Piracy

- ▶ **Congress should impose criminal penalties for acts that lead to widespread copyright infringement**, punishing not only the act of infringement, but also the steps leading up to infringement, such as acquiring in-the-clear copies without authorization or registering for peer-to-peer networks under a false identity to evade prosecution;
- ▶ **Congress should modify the laws governing computer hacking to allow content producers to fool potential pirates with decoy files.** Flooding peer-to-peer networks with annoying files disguised as sought-after content will make the process of piracy more difficult and encourage individuals to purchase their content legitimately;
- ▶ **Congress should not interfere with the ability of rights holders to identify and prosecute pirates.** If online piracy is to be deterred, the rights holders must be able to identify the perpetrators and initiate legal action.
- ▶ **Government, industry, and educational institutions should work together to educate the public about piracy.** Many people have an expectation that any information on the Internet is (or should be) free, and that expectation must be changed if online piracy is to be brought under control;
- ▶ **Federal and state laws should not discriminate against online distribution of content.** Protectionist laws that favor bricks-and-mortar retailers will only slow the digital transition and encourage users to resort to piracy to acquire what they cannot get legally;
- ▶ **Congress, rather than the courts, should lead the debate on how consumers can use digital content.** Excessive confusion over what consumers are permitted to do with purchased content creates a gray area where the culture of piracy can flourish, and Congress should lead the debate to clarify the legal uses of content;
- ▶ **The government should not restrict innovative business models for making content available to consumers.** New technologies will lead to new ways of selling content, such as self-destructing files, and the laws must not entrench analog-era notions of buying and renting content; and
- ▶ **The federal government should grant antitrust leeway to “portal sites” operated by content producers.** Digital distribution will only work if it is simple for the average user, and just as portal sites have benefited consumers in the travel industry, the content industry should be allowed to make purchase as easy as possible.

The Problem of Piracy in the Digital Era

Why is the Threat of Piracy Greater Today?

The first step in creating a set of rational copyright policies for the digital era is to determine the seriousness of the threat. Many cyberlibertarians and other advocates who oppose strong copyright protection for content contend that the protests of providers are merely the next step in a long history of resisting new technologies before embracing those technologies and finding new revenue streams.⁶

The classic example of this is the popularization of the video cassette recorder. Movie studios, afraid that inexpensive home recording would increase piracy and put them out of business, fought fiercely against the production of VCRs, eventually leading to a Supreme Court decision that a technology with “substantial noninfringing uses” cannot automatically be assumed to be a piracy device.⁷ Defeated in the legal arena, the studios ultimately embraced the VCR, creating the multi-billion dollar video rental industry and changing the price schemes on video cassettes. The result was lowered video prices (from \$80 to \$20)—which popularized the purchase of movies for home viewing. This story, and similar stories about recording technologies from piano scrolls to audio cassettes, form the basis of the argument that the threat to content from digital technologies is overblown, and time will show that content providers will ultimately profit greatly if they simply exercise imagination in their business models.⁸

Unfortunately, in this case the past is unlikely to be prologue. **Digital recording technology and the Internet represent a quantum leap forward in piracy tools. Previous worries about widespread piracy may have proven to be exaggerated, but this time the magnitude of the threat is beyond anything that has come before.** There are a number of differences between previous generations of recording technology and the new technologies that make piracy significantly easier today.

Perfect and Inexpensive Replication

In the past, analog recording technologies such as audio and video cassettes had a built-in check on widespread piracy: The quality of the recording degenerated significantly with each new generation. If a cassette was purchased at the store and copied on a home stereo, the resulting “first generation” copy was slightly degraded but still quite good. If that first generation copy was used to create another copy, the quality of the second generation copy declined precipitously. Generally speaking, in both audio and video cassettes, the quality of third-generation copies was so poor that most consumers preferred to pay for a pristine copy than get a degraded copy for free. Moreover, the replication media in some cases were more expensive and time-consuming than buying a legal copy, particularly regarding books (which are less expensive to purchase than to photocopy at the library).

These technological limitations on copying do not exist in the digital world. Each copy of a digital audio or video file is exactly as good as the original from which it was made.⁹ Thus, a single high-quality file can begin a copy cycle that grows exponentially, as each subsequent copy generation spawns new generations of copies that are just as good as the original. Once a consumer has invested in a personal computer and Internet connection, each copy is virtually free.¹⁰ While this is an important step forward in the legitimate distribution of content, it also means that the opportunities for piracy are greater than ever before.

Internet Distribution

In the past, the only way to get a pirated copy of a song or video was to come into physical contact with somebody who already had a high-quality copy. Though some pirates set up booths at swap meets and on street corners, in general someone seeking a pirated copy needed to have

a personal friend who had already purchased the original. This served as a natural break on piracy, as it was frequently easier to buy a cassette than to seek out somebody who had paid for it and was willing to make a copy for free (or at least the price of a blank tape).

The Internet has changed that forever. Napster and its successors—KaZaA, Morpheus, and other file-copying software—allow anonymous individuals around the globe to connect and obtain files or make them available for copying to anyone in the world. The software itself does not make the copies; the simple act of downloading a file from another computer is the copy mechanism. Rather, these programs serve as massive, real-time search engines, allowing individuals to search millions of networked computers simultaneously for certain files and connect them for download automatically.¹¹ Thus, it is no longer necessary to know someone who purchased a factory-produced song or video to get a pirated copy; so long as one person out of the millions on the network has it, it can be found and copied in minutes. These programs also make file copying easier by allowing the pirates to remain relatively anonymous; short of a court-issued subpoena to an Internet Service Provider (ISP), it is virtually impossible to identify individuals engaged in copying.

File Copying Instead of File Swapping

One of the biggest misconceptions in the digital copyright debate is the idea that copying that occurs on Napster-like services is “file swapping” or “file sharing,” instead of what it truly is—file copying. This is an important distinction, because true “swapping” or “sharing” is protected under current copyright law under a doctrine known as the “first sale” doctrine.¹² Under this doctrine, a person is entitled to “sell or otherwise dispose of” a legally obtained copy of a work, forming the basis for an entire industry of stores selling used books, records, movies, and video games. However, the first sale doctrine only applies to true swapping or sharing; that is, the person who owns the copy must surrender it in order to get a different copy or cash in exchange. The key is that this doctrine applies to a *particular* copy, but does not give consumers the right to make and pass along additional copies of a work on their own.

In the digital environment, that element of swapping or sharing no longer exists. When a file is swapped or shared over the Internet, the original owner retains the original copy. It is as if someone went to a used bookstore looking to trade one book for another, but got to leave the store with both books. Needless to say, this goes beyond what was envisioned in the first sale doctrine. If file swapping over online services meant that a downloaded file disappeared from the computer of the original owner, that activity would be more in line with what Congress envisioned in creating the first sale doctrine. That is not the way it works, however, and though it is possible to create file swapping software that works in a manner consistent with the first sale doctrine, it is very unlikely that this particular genie will be put back into the bottle.

Viral Spread

One implication of the perfect replication and easy Internet distribution of the current era is that a file can spread like a virus. One unprotected copy can lead to two, which leads to four, and so on until the file has spread around the globe. This means that it is no longer good enough to keep a very tight technological lid on copyrighted content.

Even if content is protected with the best copy protection technology, “in-the-clear” copies can still find their way to the Internet.¹³ These copies sometimes come from within—employees of the record labels or movie studios steal the content from the inside and make it available on the Internet. Movies can be copied by pointing a digital camcorder at a movie screen. High-quality copies of songs and videos can also be created on playback. For instance, by placing a microphone in a soundproof room and playing a song on an expensive stereo system, a reasonably high-quality copy can be made; though this method of copying requires significant expense and effort, “viral spread” means that only one person needs to be willing to do this and the file is forever available.¹⁴ Because potential pirates are everywhere in the production and distribution chain, and because no copyright protection scheme is perfect, the reality of viral spread undercuts even the best copyright protection technologies. Digital piracy, therefore, is a problem that can never be fully solved, merely managed.

Culture of Piracy and the Expectation of Free Information

This is perhaps the most troubling aspect of the copyright problem in the digital era: Many otherwise law-abiding citizens who would never even consider shoplifting a CD from a store at the mall see nothing wrong with downloading music for free. Indeed, the wide availability of music on the Internet has created a culture where some consumers justify illegal copying as a rebellion against “greedy corporations.”¹⁵ One reason for this is that users have come to expect the Internet to provide content for free that would be paid for in the offline environment, such as newspapers and magazines. Another reason is that consumer-oriented media products closely tie the content and the media together, allowing consumers to mistakenly assign the value to the media itself. Consumers may believe, therefore, that the DVD itself is the expensive item that is morally off limits for theft, but the movie recorded on that disc is an unlimited resource which is acceptable to take without paying. This, of course, is a gross misconception.

The culture of piracy is also fostered by the anonymity of the Internet. Because there is little risk of detection, even those consumers who fully understand that it is wrong to download content without paying for it will do so anyway. The fact that millions of others are doing it as well, without ever needing to face the consequences, reinforces the attitude that the person doing the stealing is just one of a faceless crowd who will never get caught.

In addition, the culture of piracy is encouraged by a significant number of cyberlibertarians who espouse an ideology that denies the legitimacy of the concept of copyrights, preferring instead to think information cannot be property.¹⁶ Less extreme are legal scholars, such as Berkeley law professor Pamela Samuelson and Stanford law professor Larry Lessig, who employ rhetoric about fair use and the limits of copyright law to create a general sense that the widespread file copying taking place on peer-to-peer networks is somehow more legitimate than efforts to stop the piracy from occurring.¹⁷ Added to that are cybervigilantes who feel that the major labels and studios have colluded to keep prices high in the past, and piracy is a justified response to what they see as

corporate malfeasance.¹⁸ Taken together, there is a widespread culture of digital piracy that to date has not been countered with social opprobrium—a clear and unambiguous signal that downloading content for free is wrong.

How Can Content Be Stolen?

One frequent misconception about the growth of digital technology for distributing content is that it can simply be matched by equal advances in copyright protection technology. Just as Macrovision served as a fairly effective protection for video cassettes in the analog environment, digital technologies should be able to protect digital content.¹⁹ This is not necessarily the case. Determined pirates have many methods of making illegal copies, and Internet distribution and viral spread take over to make the content widely available. Moreover, hackers and thieves seeking to steal digital content can usually move more quickly than the multi-industry task forces that must come together to create copy protection technologies.

Simple “Ripping” and Copying

The easiest way for pirated content to be made available on the Internet is to “rip” a CD or DVD. Doing so involves varying degrees of difficulty. For example, DVDs have been protected from the outset by encryption technology that prevents unauthorized access and copying. Because the Digital Millennium Copyright Act (DMCA) makes it illegal to circumvent such access control measures, hacker-created software is necessary to get in-the-clear copies. (This software is widely available for download on the Internet.) At the other end of the spectrum are files like older music CDs that contain no copy protection; software to rip the files into downloadable format is widely available from commercial producers. In other cases, such as programs broadcast on pay cable channels, the content is protected by “conditional access” technologies to ensure that it cannot be viewed by non-subscribers, but is essentially in-the-clear when received by a paying customer and is thus vulnerable to being digitized and posted on the Internet.

In all cases, of course, making the files available online in a peer-to-peer network is illegal. Most

people who make copies of content do not care if it is legal or not, because the chance of getting caught and punished is so low. As discussed in more detail below, the technical hurdles presented by copy protection schemes are rarely a major concern either; hackers routinely crack encryption and distribute files.

Exploiting the “Analog Hole”

Though most content is now sold to consumers in digital format, most of the playback devices—speakers, monitors, television sets—are still analog devices. Therefore the digital-to-analog (D/A) converter is a primary component in every multimedia device. Since most copy protection schemes are digital, and because the digital protections are generally lost when a digital file is converted to analog format for viewing, this creates an “analog hole” in digital copy protection schemes whereby the signal can be captured after conversion to analog and then redigitized in an unprotected form using a readily available analog-to-digital (A/D) converter.

This is a relatively simple option for those who don’t have the skill or inclination to circumvent standard copy protection. Though doing so involves some degradation in quality, the resulting copy is more than serviceable, and after the initial redigitization, future generations of copies will experience no further degradation.²⁰

Capturing Rendered Content

Even if a device features copy protection on all the digital and analog outputs, the content must ultimately be displayed in-the-clear so the consumer can see it or hear it. This means that pirates can get a copy of otherwise encrypted material simply by putting a microphone up to a speaker or pointing a video camera at a television screen. Of course, this can involve a serious degradation in quality—an entire episode of *Seinfeld* focused on the ridiculous effort to create videos of movies in crowded theaters—but under the right circumstances, the resulting copy can be quite good: an empty movie theater (after hours with the help of theater employees) or a camcorder that is plugged into the headphone jacks for hearing-impaired patrons, can give perfect audio for a bootleg copy. Though there are some efforts underway to protect against this

type of piracy (see below), there is no certainty that the technologies will be effective and, in any case, it will be very difficult to stop this type of piracy in the short run.

What Are the Legitimate Uses for Copying Content?

The issue of illegal file copying might not exist if all copyright owners employed military grade encryption and required consumers to play the content on special devices that made direct copying impossible. There are reasons, however, to encourage the development of advanced copy protection schemes that provide meaningful protection for copyright owners while at the same time allowing flexibility for consumers. For example, there are several legitimate reasons that content might be copied and used without violating copyright law. Locking up content behind airtight technological walls—to the extent that this is even possible—would make those legitimate uses much more difficult, and anger consumers who have come to expect through decades of use that they will be allowed to make copies under certain circumstances. Additionally, such measures raise the price of content for law-abiding consumers.

Fair Use of Content

The fair use doctrine²¹ is commonly misunderstood and frequently misapplied in the digital copyright debate. Fair use is rather complicated and applies a four-part test to a particular use to determine whether it infringes a copyright.²² In general, however, fair use is designed to protect specific non-commercial uses of copyrighted material, primarily for educational purposes (i.e., a teacher may incorporate a clip of a historical drama into a classroom presentation) or purposes of criticism or news reporting (i.e., someone writing a review of a new novel may quote passages of the novel for discussion). Fair use does not mean, as is commonly supposed, that any copying of copyrighted content is permissible as long as the person doing the copying does not intend to profit from it.

At the same time, fair use remains an important part of the balance struck in copyright law. The fundamental theory underlying copyright is that granting a creator monopoly rights over a creation

will encourage innovation and imagination. That monopoly, however, must have certain limitations for creativity to flourish, and fair use is one of these.²³ Protecting content from digital tools that make widespread piracy simple while allowing easy access to content for fair use purposes is a primary challenge of copyright policy in the digital era. **It is important, however, to remember that fair use is a balancing factor to copyright, and not an absolute right or a good that must be valued above all others.**

Technological Efficiency

Another common reason for copying digital content is to make the use or transmission of that content easier. For example, many large-scale video games sold for home computers can be copied from the CDs on which they are sold to the hard drive of the computer, which makes the games work better. This, however, can also make it easy to install a single copy on multiple machines, generally violating the terms of the license and therefore constituting copyright infringement.²⁴ Many ISPs also cache copies of frequently requested files on local servers to make Internet traffic run more smoothly for their customers. (The DMCA includes a provision to limit the liability of ISPs that engage in caching under certain circumstances.)

Congress has recognized the importance of allowing for copies that do nothing more than improve technological efficiency, and has granted an exemption for “ephemeral” copies of works made by broadcasters, webcasters, and distance educators.²⁵ Content providers themselves also recognize the importance of allowing these uses, and often account for them in their licensing terms. However, fear of piracy may overtake this generally accepting attitude toward copies that enhance efficient operation, and protecting this usage is another key challenge for public policy.

Consumer Expectations

Dating back to the sale of the original phonograph machines, consumers have spent decades building up certain expectations of what they will and will not be allowed to do with the content that they purchase. Technology has changed certain expectations over time; home recording technology, for example, is relatively recent and as discussed above, the rise of Napster and its successors have created an unfair expectation of free music available online. In general, however, most consumers have grown comfortable with a set of reasonable uses of content and are angered when their expectations are not met.

One example of copyright protection clashing with consumer expectations is the sale of music CDs that can be played in stereo equipment, but not home computers.²⁶ This prevents illegal ripping of songs, but also confuses consumers who expect that they will be able to play legally purchased CDs as they work at their computers. Some other widespread consumer expectations for content include device shifting (i.e., being able to purchase and download a song to play on a portable digital music device rather than just on the computer to which the song was downloaded); place shifting (i.e., purchasing a downloaded movie to watch both in the living room and in the back of the minivan); and time shifting (i.e., being able to record a television broadcast to watch at a later time). These expectations have varying degrees of legal protection,²⁷ but as a practical matter, **any successful business model, and indeed copyright law itself, must account for reasonable consumer expectations on the use of the content; failing to do so will only invite piracy.**

Meeting in the Middle: Encouraging Purchasing Over Piracy

Working from one essential assumption—there is no way to stop high-quality illegal copies from being distributed on the Internet—the challenge for policymakers and industry is to create a system like the one displayed in Chart 1. If getting an illegal copy is difficult and full of risk, and purchasing a legitimate copy is easy and reasonably priced, most consumers will choose to pay. The trick will be to blend a set of policies and business models to create the phenomenon displayed in the chart—discouraging piracy and increasing incentives to purchase content—while maintaining the balances inherent in copyright law.

Making Illegal Copying More Difficult

In order for content providers to continue charging for their products, the legitimate copies must have some advantage over the free (i.e., pirated) copies. That advantage can be created by increasing the hassle of free downloading, the risk of legal penalties for piracy, and the social opprobrium associated with piracy. There are several tools that help meet these goals, and meet them more effectively when accompanied by public policy levers.

Using Technology to Make Illegal Copying More Difficult

There are a number of technology options to protect copyrights in the digital environment, with varying support among the many players in business and policy. None are ideal solutions in the sense of being highly effective at a low cost with little degradation in performance. The high number of copyright loopholes and the complexity of the technology make a “silver bullet” solution highly unlikely, if not impossible.

Efforts to develop effective copyright protection technology will work to the extent that the interests of the content producers and the

device makers are aligned—both want more content available for sale. However, the incentive to find a solution breaks down if the content providers place too many technical demands on the devices or attempt to limit innovation in media playback devices. By the same token, the incentive to cooperate breaks down if device manufacturers insist upon solutions that are too weak to effectively fight digital piracy. If the right balance is not struck, the incentive for device manufacturers is to stick with the status quo for as long as possible. Complicating this problem is the presence of self-styled consumer advocacy groups made up of cyberlibertarians who want a massive overhaul of copyright law to cut back on intellectual property rights in the digital environment.²⁸

From a societal perspective, technology solutions should be evaluated with a three-point test: cost to consumers, impact on device performance, and effectiveness. Solutions that are cheap, easy to implement, and highly effective at limiting piracy should always be given priority. In the end, it will be necessary for all parties to compromise on each of these three points if a realistic solution is to be found. To the greatest extent possible, the compromises should come equally from all three categories; it is not a solution to implement copy controls that only marginally decrease digital piracy, or place an enormous cost on consumers to protect intellectual property owners from theft.

Encryption. Broadly speaking, encryption is any technology that scrambles or otherwise makes content unusable unless the consumer possesses the decryption keys necessary to access the content. Use of encryption technologies, from cable descrambler boxes to the Content Scramble System (CSS) on DVDs, is a longstanding strategy for protecting content.

The primary problem with encryption as a solution to piracy is that it requires the content companies and the technology companies to work together. Unlike many other forms of content protection, encrypted content cannot be

sold to consumers unless the playback devices are designed to decrypt it (or unless the encryption has been hacked). Because the content creators and the device manufacturers need each other to sell their products, encryption as a strategy takes widespread cooperation across multiple industries.

This need for cooperation was the drive behind the Consumer Broadband and Digital Television Promotion Act, commonly known as the Hollings Bill for its primary sponsor, Sen. Fritz Hollings (D-S.C.).²⁹ The Hollings Bill would have required the content industries, the hardware/software industries, and consumer groups to come together to create security system standards and encoding rules for use in the protection of digital content, and then require that all future digital media devices comply with those standards. If the groups did not agree on standards and encoding rules within a year, the federal government would create the standards.

This proposal was highly controversial (and subsequently died a quiet death). The idea of government-designed and -mandated security system standards bothered many critics on philosophical grounds, but equally widespread was skepticism that any content protection scheme (especially a government-mandated one) could be made tamper-proof, as previous efforts had all proven vulnerable to attack. For instance, the CSS system on DVDs entailed full cooperation, because any manufacturer who wished to build DVD players had to incorporate CSS as part of the agreement to license the technology. However, the CSS system was cracked by a teenage hacker, and the code for doing so (called DeCSS) became widely available on the Internet—though most people still refrain from copying DVDs because it is easier to buy a DVD than it is either to use DeCSS to crack a DVD or to download a cracked DVD.³⁰ Similarly, a major industry consortium called the Secure Digital Music Initiative (SDMI) was formed to create copyright protection measures for digital music. The consortium faced much internal disagreement on a variety of subjects, issued a high-profile challenge to hackers to crack their system (which the hackers claim they did), and has since quietly faded away.³¹

Another problem with encryption technologies is that the encryption disappears once the digital content is converted to an analog signal for playback on media devices (the vast majority of

which are still analog). This brings the analog hole problem into play. An encrypted cable television signal, for instance, is decrypted with a cable box and can then be transferred and copied through the analog output jacks on the consumer's media devices. The easiest way to get around this problem with such "legacy" equipment is to deliver content in a way that won't work on older devices, forcing consumers to either buy new all-digital equipment or add new technology to their existing devices. This will be expensive, and would meet with tremendous disapproval from consumers who have recently invested money in high-end media equipment. Another solution would be to redesign all analog-to-digital conversion devices to take advantage of the new Digital Rights Management (DRM) technologies, a proposition strongly opposed by some companies because they believe it will degrade the performance of the devices.³² Because the analog hole will remain until most of the existing "legacy" equipment is no longer functional (which could take decades), content providers point out that a solution needs to be devised as quickly as possible to reduce the number of unprotected devices that are on the market. The industries, at the urging of House Commerce Committee Chairman Billy Tauzin (R-La.), are currently at work trying to devise a voluntary solution to the problem.

Encryption remains an effective deterrent against unauthorized copying by the average user, but as discussed above, does not address the problem of the availability of illegal copies. Several industry consortiums, including the Copy Protection Technical Working Group (CPTWG, pronounced C-P-Twig), the Digital Video Broadcasting Project (DVB), the Moving Pictures Experts Group (MPEG), and many others are actively working on effective content protection technology for a variety of digital media. Such cooperative efforts are a key part of making piracy more difficult.

Watermarking and other embedded control technologies. The term watermarking encompasses a variety of technologies, but the basic idea they share is a small piece of code embedded in the digital data stream that will survive the transition from digital to analog and back. Some "forensic" watermarks are designed to reveal the original source of a digital file, making it easier to hunt down and prosecute

pirates. Other watermarks are embedded with the audio or video stream to convey copy protection and usage information to the playback device or the devices used to receive the signal (such as television receivers or high-speed modems).

Another type of embedded control technology is the “broadcast flag,” a signal designed to be embedded in over-the-air broadcasts of digital television and prevent copies of the broadcasts from being distributed on the Internet (as currently designed, it does not prevent home copying of television signals). Consumer groups worry that the broadcast flag could eventually be used to prevent not only illegal file duplication, but otherwise permissible network transmissions, like moving a recording from one digital video recorder to another located within the household. The Broadcast Protection Discussion Group of the CPTWG released a report on possible implementation of the broadcast flag, but the conclusions were not unanimous.³³ The Federal Communications Commission is currently considering public comments on the broadcast flag issue, and may advance a regulation that they hope will encourage the content industries to embrace digital television more quickly.³⁴ Sen. Sam Brownback (R-Kan.) has circulated draft legislation that would (among other things) prohibit the FCC from requiring a specific technology solution for the broadcast flag, but rather set objective performance standards so that any device that meets the goal of the broadcast flag is compliant.³⁵ A flexible solution such as this is the best way to implement a broadcast flag because it allows for the flag to be embedded in the signal and requires device manufacturers to read the flag but does not mandate the specific technology that does so.³⁶

Forensic watermarks, on the other hand, are a true stand-alone technology; that is, the function of watermarks is not impaired even if there is no cooperation from device manufacturers. But forensic watermarks obviously are not a complete solution. Given enough time, talented hackers can strip some kinds of watermarks from digital signals. Even if the watermarks remain intact, they make it easier to hunt down pirates but do little to prevent the piracy in the first place. **Still, watermarking can be an important part of the solution if the implementation is simple, inexpensive, and does not degrade the performance of equipment.**

Spoofing. Spoofing is a broad term for self-help efforts by content owners that exploit the anonymous nature of file sharing software.³⁷ When a user logs on to KaZaA or similar programs, they can search millions of computers for a particular file, then download the file and play it. However, the downloader does not know much about the person from whom the file is being copied.³⁸ Spoofing (or decoying) is when the content owners post fake copies of their content, flooding the network with files indistinguishable from pirated copies of the real thing. **The flood of spoofs makes finding and downloading a pirated copy much more time consuming, as the downloader is forced to wade through a sea of fakes to find a clean file.**

Spoofing encompasses a spectrum of progressively more aggressive efforts against downloaders. At its most benign, spoofers simply waste the time of downloaders by forcing them to download multiple files until they find an actual pirated one. With a sufficient flooding of the network, this can encourage downloaders to pay for a legitimate digital download, which they know will be the correct file on the first try. Unfortunately, file sharing networks tend to be so massive that a flooding spoof attack is unlikely to be effective over the long haul.³⁹ Further along the spectrum are spoof files that look like music or video files to the untrained eye, but actually contain computer code that can do a number of things—launch a web browser directed to a site where the content can be purchased legally, call back to the content provider to identify the downloader, delete other pirated files on the hard drive, or even freeze up the computer and require the user to restart the machine.

Some of these more aggressive spoofing strategies are currently prohibited by anti-hacking laws, but Rep. Howard Berman (D-Calif.) introduced legislation last year to allow certain aggressive spoofing strategies.⁴⁰ Sen. Orrin Hatch (R-Utah) went even further, suggesting that damaging the computers of pirates “may be the only way you can teach somebody about copyrights.”⁴¹ The content industries, however, have shown no interest to date in more aggressive strategies (as opposed to the unquestionably legal decoy strategies), which led Rep. Berman to abandon his bill. In any case, spoofing definitely increases the hassle of finding pirated content, and in some cases may significantly increase the

risk of doing so, which discourages piracy in favor of paying for content. More important, aggressive spoofing impacts only those users who are searching for illegally copied files; it has no impact on law-abiding users.⁴² The use of spoof files that are annoying but do no damage to a machine should be protected by law.

Using Enforcement to Make Illegal Copying More Difficult

As with all property protection, owners of copyrighted content can turn to both civil courts and the criminal justice system when their property is damaged or stolen. However, the enforcement option has always been time-consuming and expensive, making it undesirable except for the worst offenders. With the explosion of file copying enabled by the Internet, however, enforcement must become part of the overall strategy to combat piracy. Without effective tools for finding and punishing pirates, copyright holders have only two other options: lock up content using excessively strong methods or refuse to make the content available at all. Either solution ends up punishing law-abiding consumers rather than the individuals who are the cause of the problem.

Prosecution of Pirates. Though it is illegal to pirate copyrighted material, prosecutions against individuals have been few and far between.⁴³ Content owners have instead focused their legal efforts on the peer-to-peer networks, without which widespread piracy would be much more difficult. Despite the potential negative public relations involved in suing customers, content providers are starting to do just that.

Though there are millions of individuals using peer-to-peer networks for file copying, the content owners can get reasonable results by focusing on those who are making files available for copying. Most people who pirate files on the Internet are willing to download the files, but do not set their software so the files can be uploaded. (Some software comes with the upload option turned on as a default, but many users turn it off to save bandwidth for downloads.) One study of the Gnutella system showed that 70 percent of the users online did not make their files available for sharing, and that 50 percent of the “hits” to user queries were returned by the top 1 percent of file sharers.⁴⁴ The problem is so bad that some

current generation networks have tried to attack this problem by rewarding users who make files available for upload with better network performance. In theory, therefore, attacking that top 1 percent could drastically reduce the piracy on a network, and going after the top 30 percent could effectively destroy the network. Better education about peer-to-peer software can also have an impact on those who do not realize that they are uploading songs to other users because they do not fully understand the default settings of their software.

Unfortunately, going after those uploaders is difficult, because peer-to-peer software allows for anonymous connections, and finding the true identity of the uploader is a difficult and costly undertaking. The DMCA created a streamlined process for content owners to compel an ISP to turn over identity information on known pirates—it requires the information be revealed with a special subpoena issued by a court clerk rather than forcing the rights holder to file a “John Doe” lawsuit and get the approval of a judge for the subpoenas through a full-blown legal proceeding (a more expensive and lengthier task).⁴⁵ That provision underwent an unsuccessful court challenge by Verizon, which argued that the risk to individual privacy outweighs the rights of copyright owners to know the identity of thieves.⁴⁶ Without a veil of anonymity to protect uploaders from lawsuits, behavior may well start to change as more subpoenas are issued. Of course, going after downloaders is perfectly within the rights of copyright holders as well; in both cases, the increased risk of being punished for copyright infringement makes paying for content more attractive.

In September 2003, the Recording Industry Association of America (RIAA) organized a series of lawsuits against some of the most egregious peer-to-peer pirates, many of whom had in excess of 1,000 pirated song files on their computers. **Though RIAA suffered an enormous amount of bad publicity (and even condemnation from elected officials) for these actions,⁴⁷ the procedure is exactly what is necessary to stop individuals from engaging in massive piracy.** The individuals targeted by the lawsuits were generally warned in advance (by instant message, in some cases) that they were being watched, and RIAA has given users the opportunity to delete illegal song files and forswear future piracy in

exchange for a pledge from RIAA not to sue.⁴⁸ Contrary to much of the public reaction, these lawsuits do not go too far in stopping piracy; they are a measured, reasonable response and are the best option available for increasing the risk and inconvenience of piracy—the suits rightly put the enforcement burden on the property owners and the risk of punishment on the pirates, while sparing law-abiding citizens from intrusive or expensive copyright protection programs.⁴⁹

Prosecution of Peer-to-Peer Networks. The most famous case of legal action against a peer-to-peer network was the lawsuit against Napster, the file sharing software that brought music file copying into the mainstream.⁵⁰ Though legal action eventually brought Napster down, the more decentralized nature of the successor peer-to-peer networks makes it harder to stop them through legal action; a recent court ruling held that two distributors of current generation file sharing networks cannot be held legally accountable for the infringement of their users. While that decision is still under appeal, it highlights the difference between Napster and new peer-to-peer networks: Whereas Napster operated centralized servers under the control of the corporation, current file copying programs such as Morpheus and KaZaA are decentralized, passing queries from user to user rather than through one main server. That means the companies themselves merely distribute the software, but do not participate in the act of copyright infringement the way Napster did. Though the legal battle is far from settled and many outcomes benefiting rights-holders are possible, it is unlikely that lawsuits will see the same unqualified success against this current generation of software that occurred in the Napster case.⁵¹

Of course, there are also legitimate uses of peer-to-peer networks, most notably for trading media files with the permission of the producer. Garage bands and aspiring filmmakers take advantage of peer-to-peer networks in the hopes of becoming famous, and corporate networks can use such networks to manage their files more efficiently. Because of the substantial noninfringing uses of peer-to-peer networking, it is impossible as a policy matter to simply eliminate the file sharing services, although some amount of regulation might help.⁵²

Policy Recommendations for Making Illegal Copying More Difficult

- 1. Congress should give the industry standards-setting process a chance to work.** In the absence of a market failure, it is generally best to let the industry players work together to establish technical standards. This allows the greatest freedom for innovation and balance between competing interests. This principle is especially true in the case of protecting copyrighted digital works, because the challenge is so daunting and the risks are so high. There are no off-the-shelf technologies to resolve the bundle of digital copyright problems; research and development are still needed. As discussed above, it is possible in this case that the interests of all parties will not align sufficiently for a voluntary process to work in a timely manner, or worse, that the technology is simply not capable of preventing large-scale piracy while meeting the three-point test of low cost, low performance degradation, and high effectiveness. If it becomes clear that the technological problems can be solved and yet no agreement is forthcoming, it may be necessary for Congress to intervene in the process by altering the incentives of the negotiating parties to arrive at a solution within a mandated time frame. However, it is not yet clear that the voluntary process has been given sufficient time to act, and the short one-year deadline of the Hollings Bill diverted resources to the legislative battle that could have been spent in the standards-development process. Congress should step back and let current industry groups work toward establishment of solutions, while keeping close track of ongoing progress.
- 2. Once industry-led standards are developed, Congress should mandate the solutions.** The main downside to a voluntary process is that some manufacturers (particularly those based overseas) have an incentive not to comply with the copy protection scheme endorsed by the industry—devices that enable piracy would have a unique selling point. While the federal government should avoid being the body that sets the standards, it is entirely

appropriate for Congress to mandate compliance with a privately-set standard to eliminate free-riders—those who take advantage of the increased availability of digital content to sell their equipment without accepting responsibility for protecting the content from pirates.

3. **Congress should criminalize the tools of piracy as well as the actual infringement.** The process of copyright infringement is not limited to the simple act of downloading a song or movie from a peer-to-peer network. There are several steps that precede that final result, and Congress should act to intervene in those steps. This is the logic behind the anti-circumvention provisions of the DMCA—the first step in a pirated download is frequently the hacking of a copy protection system. In addition to hacking, there are plenty of other tools and methods that pirates use to generate in-the-clear files and make them available to downloaders. A group of House Democrats, led by Judiciary Committee Ranking Member John Conyers (D-Mich.), introduced legislation that would attack some of these earlier steps.⁵³ The bill would, among other things, create criminal penalties for recording a film as it is displayed in a theater and for giving false information when registering an Internet domain. Attacking piracy at these earlier stages will decrease the amount of pirated material in the pipeline and lessen the pressure to find technological solutions.
4. **Congress should not interfere with the ability of rights holders to identify and prosecute pirates.** In the wake of a flood of bad publicity following the RIAA's first wave of lawsuits, many interest groups and even some elected officials began complaining loudly about the process and suggesting changes that would tie the hands of rights holders. The proposals range from reducing the potential liability of the pirates—some individuals could have been sued for millions of dollars—to changing the DMCA to make it more difficult for rights holders to discover the identity of peer-to-peer users.⁵⁴ Congress should resist this rhetoric. The risk of legal action against online pirates is already very slim due to the sheer volume of illegal downloading occurring on the Internet today. Reducing the risk even further would be counterproductive to the goal of making legal purchases easier than stealing content. Moreover, reducing the tools that content holders have to go after illegal downloaders would increase the pressure for copyright solutions that would impinge on the millions of law-abiding Americans who do not illegally download music.
5. **Congress should clarify the federal computer hacking laws to permit more aggressive spoofing efforts that do not damage devices.** Though Rep. Berman (D-Calif.) declined to reintroduce his bill amid howls of protest by the Internet community, he was on to a good idea. Allowing content owners to take steps to disable file copying through the use of spoof files would help to discourage such piracy. Though the language of any such law would have to be carefully worded to prevent damage to machines and Internet infrastructure, the very knowledge that any downloaded file could turn out to be a relatively benign but extremely annoying spoof would make the peer-to-peer networks riskier places to acquire music and video files. Though no content providers are currently pursuing such a strategy, it may become necessary in the future as the piracy problem becomes worse, and a firm legal footing for doing so should be established now.
6. **Government, industry, and educational institutions should work together to educate the public about piracy.** Because stealing copyrighted material is becoming easier than ever in the networked digital environment, the culture of piracy is taking root in a more damaging way. Journalists carry a certain amount of responsibility for this, by portraying a “balanced” view of the issue that gives the pirates credibility equal to the artists who create the work. Colleges and universities also bear responsibility, as they have largely treated massive piracy on campus networks as a bandwidth issue rather than a criminal activity issue. (It is as if administrators were to attack drug dealing in college dormitories because it causes traffic jams on campus.) The attitude that

downloading content without paying for it is acceptable must change, and all interested parties—including artists in the entertainment industry—should work together to communicate this message.

Making Purchasing of Content Easier

No matter how risky or inconvenient it is to find pirated files on the Internet, Napster-like programs will remain popular unless downloadable content is easy to access and reasonably priced. The success of Apple's iTunes service, which sold over one million songs at 99 cents each in its first week of operation, shows the tremendous demand for legal downloadable content. There are three keys—both public and private—to accomplishing this goal.

Passing the Savings from Content Providers to Consumers

The physical distribution of digital content on CDs and DVDs—the manufacture of the disc, printing, packaging, shipping, and retail markup—is a significant expense, accounting for more than half of the cost of a music CD.⁵⁵ (The percentage varies by industry based on the initial content production costs.) Selling content over the Internet replaces these costs with less expensive e-commerce costs, but initial business models (especially in music) planned to sell downloadable versions for the same price as the physical copies.

That pricing decision cannot be blamed entirely on greed or shortsightedness (though both may have played a part). Rather, the content industries are facing the same barrier that other industries have faced in making the slow transition to e-commerce: the bricks-and-mortar retailers. The middlemen responsible for selling the physical versions of the product do not want to be undercut by a website selling the same thing for much less, and since the retailers will continue to represent the vast majority of total sales in the early stages of the transition, the content companies must tread carefully to protect their primary distribution outlets. This is a problem already faced by toy manufacturers, book publishers, and other companies that sought to sell their products online and eliminate the middleman. **At the extreme, middlemen have**

used their political influence to strangle online competition, as has happened in the contact lens industry and the automobile industry, or have filed lawsuits, as the National Association of Recording Merchandisers did to Sony to prevent advertising of Sony's e-commerce site in music CDs.⁵⁶

No matter the root causes, the end result is clear: Sales of music have fallen dramatically. As high-speed Internet connections proliferate, the same fate is likely to befall the video and software industries if they make the same business decisions. Digital distribution can change the economics of content sales, making customers feel they are getting a better value for the amount spent if the savings from eliminating the middlemen is shared with them.

Giving Consumers Flexibility in Content Use

A major reason that consumers favor physical distribution over digital distribution is that the old model of purchasing a hard copy at the mall comes with a predictable and flexible set of options: letting a friend borrow the disc for an evening, playing the disc in both the computer and DVD player, making "mix tapes," and so on. Most digital distribution models, in their zeal to prevent illegal file sharing, placed considerable restrictions on what could be done with the files. In the most extreme (yet very common) example, digital music was sold as a subscription service that could only be streamed to a computer that had a live Internet connection. With such restrictions on use, it is little wonder that consumers turn to the peer-to-peer networks—including those who would gladly pay for the music if they could get it the way they wanted it.

This flexibility is so important in the marketplace that there have been numerous calls to mandate it for digital downloads. A group called DigitalConsumer has proposed a "Consumer Technology Bill of Rights" that includes a number of flexible uses, such as time shifting digital television broadcasts (recording to watch later) and the right to play legally acquired content on any device.⁵⁷ Rep. Zoe Lofgren (D-Calif.) has introduced the Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act to define many of the same rights, including repealing an anti-circumvention provision of the DMCA that

will allow consumers to circumvent copyright protection schemes if the use of the content after circumvention is otherwise legal, such as playing a DVD on a computer using a non-Windows operating system.⁵⁸ Sen. Ron Wyden (D-Ore.) has taken a less aggressive approach in the Digital Consumer Right to Know Act, which requires content providers to disclose the limitations imposed by copyright protection measures to consumers before purchase.⁵⁹ Though these approaches differ, and while there is disagreement on whether they would achieve their stated aims, the unifying principle is a desire for consumers to have their expectations met with regard to their ability to use digital content while protecting copyright holders from rampant digital piracy.

Of course, some restrictions on the use of digital files will be necessary to ensure that the content providers aren't simply offering a "honey pot" of high-quality digital files that are then freely traded on peer-to-peer networks; new technologies call for new protections. **However, retaining flexibility of use as close as possible to what consumers have done with content all their lives will be key to the success of digital distribution.**

Allowing Single Portal Access

One of the chief advantages to the retail system of content distribution is that most consumers remain blissfully unaware of which labels or studios produce the music and movies they buy (with the possible exception of Disney, which is a brand in itself, and software, where companies trade heavily on their reputation). Consumers can simply walk into a store and look for the name of their favorite band or favorite movie and expect it to be on the shelves, no matter which company produced it. A system where all creative content was sorted by the company that produced it would be extremely ineffective, absent a revolution in the way content is marketed by the producers.

Because of this, Internet distribution will not be as effective if each company is left to distribute its products at its own websites. At a minimum, there needs to be a single portal to search for content by title, artist, and so on, even if that site then redirects the consumer to a company's online store. Ideally, however, all of the companies would be allowed (though not required) to put their wares in a single place where consumers could buy them.⁶⁰

Though industry-supported portal sites are the wave of the future for e-commerce, many companies are reluctant to become involved because of the threat of antitrust action by the federal government. The experience of Orbitz, the portal site for the airline industry, is instructive. The airlines developed a single place for consumers to search for airfares, with the condition that all participating airlines had to make their lowest fares available to the portal, a move made advantageous by the elimination of payments to middlemen in the ticketing and travel agent industries. As a result of pressure from both online and offline competitors, intense antitrust scrutiny followed, and while Orbitz continued operating until ultimately being cleared by the U.S. Department of Justice, it has been a cautionary tale for other industries.⁶¹ Indeed, the Movies.com joint venture between just two studios—Fox Entertainment Group and the Walt Disney Company—fell apart due to antitrust scrutiny by the Department of Justice.

Policymakers need to recognize that, from an antitrust perspective, collaboration by producers is different than collaboration by distributors. The primary reason is that producers build their profit margins into the wholesale cost and are not looking to gain additional profit by maintaining a high-cost distribution process; rather, the incentives on producers is to find the widest, deepest, and cheapest distribution channels for their content. In contrast, if middlemen collaborate to develop a portal, they have a stake in protecting their existing business models and extracting monopoly rents. Furthermore, not all content is created equal; some songs, movies, and video games are vastly more popular than others in a way that doesn't occur in most industries, so "products" such as Madonna are not as easily substitutable by consumers.⁶² More important, the ever-present threat of piracy (as discussed above) acts as a natural check on the pricing of content, as proven by the evolution of online music sales over the past two years. Finally, content producers who wish to distribute online face retaliation from their offline business partners,⁶³ and in such circumstances antitrust law is brought to bear as a business cudgel rather than a shield for consumers. In fact, in such instances, carefully regulated cooperation by producers can reduce retaliation by retailers.

Policy Recommendations for Making Purchasing of Content Easier

- 1. Federal and state laws should not discriminate against online business models.** There are two major elements to ensure that content providers are not unfairly burdened by protectionist policies that favor middlemen. First, states should refrain from passing laws or regulations that favor physical distribution of content over digital distribution, including taxes or retail licensing requirements that could make online distribution difficult or impossible (such as requiring a physical presence in the state to conduct business in that state). Second, the Federal Trade Commission and the Department of Justice should maintain intense scrutiny of retailers to ensure that they are not using their power as distributors to act in anticompetitive ways, such as colluding to refuse to carry products from companies that launch e-commerce services.
- 2. Congress should lead the debate on how consumers can use digital content.** Though we believe the Digital Consumer Bill of Rights and the BALANCE Act go too far, we also believe that Congress must hold a full debate and settle on “sense of the Congress” language. Legislation regarding what consumers can and cannot do with legally acquired content is premature given the uncertainty of evolving business models. Continuing under the murky fair use doctrine will not only leave important public policy decisions to the courts (where fair use decisions are made) but will also allow the cyberlibertarians to continue with their rhetoric suggesting that file copying is somehow legal. We believe some practices—like disclosure of copy protection (as Sen. Wyden’s legislation mandates)—should be widely accepted, whereas others—such as hacking console-based video games to play on a personal computer—will be more controversial. Whatever the outcome, it is vitally important that the nation’s elected
- 3. The government should not restrict business models for making content available to consumers.** When contemplating how consumers will be allowed to use content, it is important not to prevent content producers from experimenting with business models. New digital technologies are beginning to blur the lines between the concept of “owning” and “renting” a copy. Content delivered over the Internet can be set to expire like a rental or last forever like a purchased copy of a CD or book. Similarly, Disney’s new EZ-D line of DVDs are purchased like a regular DVD but “expire” after a limited time like a rental that does not need to be returned. These are experimental technologies and marketing methods, and it is unclear whether the cost and convenience of innovative licensing models will be embraced by consumers. Whatever the outcome, it should be decided by market forces and not government mandate.
- 4. The federal government should grant antitrust leeway to producer portal sites.** Portals have the potential to become anticompetitive, but they should not be presumed guilty from the start. This is particularly true of portals developed by content producers. Assuming the proper policies are in place—non-discriminatory displays of products, full product availability to other online retailers, competitive pricing, full inclusion of all industry players, and so on—producer portal sites can be very beneficial to consumers by offering less expensive and more comprehensive content libraries. Clear signals from the Federal Trade Commission and the Department of Justice as to what practices will be unacceptable can help encourage the content providers to join forces and offer their wares in a way that is easy and inexpensive for consumers.⁶⁴

Conclusion

The problem of copyright protection in the digital era is complicated; there are no right or wrong answers, only the balancing of trade-offs. Policymakers must take steps to ensure that the individuals and companies that create and distribute content have their property protected from theft. At the same time, public policy must encourage the other myriad benefits

of the digital era—technological innovation in both content and devices, disintermediation of middlemen that serve only to increase costs, and so on. By balancing these competing interests and creating an environment where content providers can take full advantage of digital technology, the digital era holds the promise of new vistas of creativity.

Endnotes

¹ <http://uk.biz.yahoo.com/031001/80/e9wfv.html>. The decline may also be due in part to other factors, such as the poor quality of contemporary popular music.

² Festa, Paul, "Latest Potter book scanned, swapped," *CNET News.com*, June 25, 2003, <http://news.com.com/2100-1025-1020984.html>.

³ <http://www.musicunited.org/>.

⁴ According to the International Intellectual Property Alliance, exports and foreign sales of intellectual property totaled about \$89 billion in 2001. <http://www.iipa.com>.

⁵ <http://www.apple.com/music/store/>.

⁶ Berkeley law professor Pamela Samuelson, one of the leading opponents of digital copyright protection, put it this way: "We should also not assume that these copyright maximalists are good judges of what's in their long-term best interest. Shortsightedness can be one of their hallmarks. It wasn't so long ago that major motion picture producers were bewailing the advent of videotape machines as the end of film revenues. They lost their battle to ban the sale of these machines—with the result that a new and unanticipated market for their products emerged in the form of videotape sales, a market that has brought further prosperity to the film industry and satisfaction to the public." Samuelson, Pamela, "The Copyright Grab," *Wired Magazine*, January 1996, http://www.wired.com/wired/archive/4.01/white_paper_pr.html.

⁷ More specifically, the manufacturer of the device cannot be liable for contributing to copyright violations because the manufacturer can't be assumed to have "knowledge" of infringement as long as the device has substantial noninfringing uses. *Sony Corp. of Amer. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). The full text of the majority opinion can be found at http://www.law.cornell.edu/copyright/cases/464_US_417.htm.

⁸ For example, one frequent proposal is to use recorded content as a promotional tool and to earn a profit on concerts, t-shirt sales, and so on. That is an unlikely business model even in the music industry, and impossible for films and other forms of content.

⁹ There is some degradation in quality based on the compression software used on files to make the file size smaller and the download time shorter. The popular audio format known as MP3 became a widely used standard because it was only slightly degraded from "CD quality" sound and made files small enough to transmit over the Internet in just a few minutes. Continuing advances in compression technology improve that trade-off even more, and the quality of digitally-copied files continues to increase while the size (and transmission speed) of the files remains relatively constant.

¹⁰ Because of limitations in bandwidth, downloading content is not perfectly free, as it can carry a heavy opportunity cost by tying up an Internet connection for many hours. However, this cost is small for individuals with high-speed connections, and file copying software can be set to download multiple files overnight or when the computer and Internet connection are not in use.

¹¹ Most of these software programs have additional features to make file copying easier, such as automatically searching for new sources to complete the copy if a download is interrupted by network problems.

¹² 17 USC 109.

¹³ For this report we will take "in-the-clear" to mean that a copy is reproducible and has had all copy protection technology removed (or never contained copy protection technology in the first place).

¹⁴ Policymakers should assume that there will always be at least one person willing to go to such effort even if that individual stands no chance of profiting from the effort; the Internet is rife with people who view stealing content as a crusade against rapacious record labels and movie studios.

¹⁵ <http://www.prospect.org>.

¹⁶ The website of the Electronic Frontier Foundation includes an article by Professor Brian Martin advancing the thesis that "most of the usual arguments for intellectual property do not hold up under scrutiny." http://www EFF.org/IP/against_ip.article.

¹⁷ Samuelson's work can be found at <http://www.sims.berkeley.edu/~pam/papers.html>. Lessig's work, including his blog, can be found at <http://www.lessig.org>.

¹⁸ In one recent case, pop star Madonna flooded the Internet with spoof files containing a vulgar scolding message to discourage downloaders from stealing songs off her upcoming album. In response to this, a hacker took over her website and posted copies of all of the songs from the album. The Smoking Gun website reports the incident in this way: <http://www.thesmokinggun.com/archive/madonnasplash1.html>.

¹⁹ For more on Macrovision and its limitations, see http://www.repairfaq.org/filipg/LINK/F_MacroVision.html.

- ²⁰ A typical technique is simply to run a cord from the analog output jack of a DVD player into a computer equipped with an A/D converter.
- ²¹ 17 USC 107.
- ²² For a concise summary of the fair use test, see <http://www.copyright.gov/fls/fl102.html>.
- ²³ Another major argument over the limitations of the rights of content creators is the extension of the copyright term, as recently embodied in the Sonny Bono Copyright Term Extension Act (P.L. 105-298) that extended many copyright terms by 20 years.
- ²⁴ Some efforts by software producers to protect against these multiple installations—such as mandating a registration of the program with the company website—have brought protests from privacy advocates and consumers.
- ²⁵ Section 112 of the Digital Millennium Copyright Act (P. L. 105-304).
- ²⁶ The “key2audio” scheme (<http://www.key2audio.com>) is one such technology, though it was reported that the copy protection could be defeated by drawing on the disc with a felt-tip marker (<http://www.wired.com/news/technology/0,1282,52665,00.html>).
- ²⁷ For example, the Betamax case enshrines the principle of time shifting, but declined to address some important implications, such as keeping a library of recorded broadcasts for repeated viewing as opposed to watching a show just once.
- ²⁸ The Electronic Frontier Foundation, for example, opposed every part of the decision on the broadcast flag. <http://www.cptwg.org/Assets/BPDG/home%20page.htm>. For more on the broadcast flag, please see the section entitled “Digital Watermarking.”
- ²⁹ S. 2048 in the 107th Congress.
- ³⁰ The DeCSS case involved the issues of both fair use (the claimed purpose of DeCSS was device shifting, so DVDs could play on computers running the Linux operating system) and free speech (the code for the DeCSS software was distributed as text, prompting court challenges under the anti-circumvention provisions of the DMCA).
- ³¹ The SDMI website (<http://www.sdmi.org>) has not been updated for nearly two years.
- ³² Leopold, George, Rick Merritt, and Junko Yoshida, “Plugging the analog hole: Intercepted signals are latest front in copy-protection wars,” *EE Times*, September 20, 2002, <http://www.eetimes.com/issue/fp/OEG20020920S0062>.
- ³³ Broadcast Protection Discussion Group Home Page: <http://www.cptwg.org/Assets/BPDG/home%20page.htm>. Of particular note are the comments of the Electronic Frontier Foundation, which are representative of the cyberlibertarian opposition to the broadcast flag.
- ³⁴ Media Docket No. 02-230; see the testimony of FCC Media Bureau Chief W. Kenneth Ferree before the House Subcommittee on the Courts, the Internet, and Intellectual Property at <http://www.cptwg.org/Assets/BPDG/home%20page.htm>.
- ³⁵ “Sen. Brownback’s proposed bill: A draft version of the Republican congressman’s legislation,” *Salon.com*, June 17, 2003, http://www.salon.com/tech/feature/2003/06/17/brownback_draft.
- ³⁶ For a detailed explanation of the broadcast flag proposal and the changes necessary to allow for a flexible compliance regime, see “Implications of the Broadcast Flag: A Public Interest Primer” from the Center for Democracy and Technology, October 2003, <http://www.cdt.org/copyright/broadcastflag.pdf>.
- ³⁷ The term *spoofing* originally referred to the practice of disguising the origin of an Internet communication, but it has taken on this additional meaning as well.
- ³⁸ The software will reveal certain technical information, such as IP address, connection speed, chosen username, and the like but does not contain an effective “trust rating” for users.
- ³⁹ Flooding a file sharing network is most effective in the period immediately before and after the release of a new song or movie, when downloaders log on hoping to find a copy leaked by someone with access to the content before the release date. Because the viral spread has not had time to take effect at this early stage, it is easier to create a high ratio of spoof files to pirate files. However, after a period of days or weeks, the pirated files have spread to a sufficient number of computers that they outweigh the spoof files, making it unlikely that any given downloader will accidentally copy a spoof file.
- ⁴⁰ H.R. 5211 in the 107th Congress.
- ⁴¹ <http://www.wired.com/news/digiwood/0,1412,59298,00.html>.
- ⁴² A widespread spoofing program would involve some externalities, as massive downloading of useless files will clog the Internet infrastructure. However, this is a self-limiting externality — if the number of spoof files being downloaded is so large that it slows the entire Internet, that would indicate that the hassle factor of downloading pirated files has gone off the chart, and people would stop trying to do so.
- ⁴³ The prosecutions vary by industry, with the software industry pursuing a particularly aggressive prosecution strategy. However, the prosecutions of all Internet content pirates to date represent a miniscule percentage of the

total piracy that occurs online.

⁴⁴ Adar, Eytan, and Bernardo Huberman, "Free Riding on Gnutella," *First Monday*, http://www.firstmonday.dk/issues/issue5_10/adar/.

⁴⁵ 17 USC 512(h).

⁴⁶ Among the claims cited by Verizon and their advocates in the privacy community is that the streamlined process under the DMCA could allow abusive men to find battered women that are in hiding.

⁴⁷ Dean, Katie, "Schoolgirl Settles With RIAA," *Wired.com*, September 10, 2003, <http://www.wired.com/news/digiwood/0,1412,60366,00.html>.

⁴⁸ RIAA refers to the amnesty offer as the Clean Slate Program: <http://www.riaa.com/news/newsletter/pdf/cleanSlateDesc.pdf>.

⁴⁹ Of course, it is expensive to file hundreds or thousands of lawsuits, and to the extent that the settlements reached in the lawsuits do not cover the costs incurred by the record labels filing the lawsuits, a burden will be placed on consumers in general. However, that burden will be relatively light compared to other options for protecting intellectual property.

⁵⁰ For more information on Napster, see "Napster and Online Piracy," by Shane Ham and Robert D. Atkinson, *Progressive Policy Institute*, May 2000, <http://www.ppionline.org>.

⁵¹ For a more complete analysis on why current peer-to-peer networks may survive legal scrutiny, see "Why Grokster and Morpheus Won, Why Napster Lost, and What the Future of Peer-to-Peer File Sharing Looks Like Now," by Chris Sprigman, *Find Law*, May 8, 2003, http://writ.news.findlaw.com/commentary/20030508_sprigman.html.

⁵² For example, PPI has recommended that peer-to-peer networks not be allowed to operate with anonymous log-ons, so the real identity of a user is available when a court order is obtained against an infringer. Ham, Shane, and Robert D. Atkinson, "Napster and Online Piracy," *Progressive Policy Institute*, May 2000, <http://www.ppionline.org>.

⁵³ H.R. 2752 in the 108th Congress.

⁵⁴ There is not yet any credible evidence that the DMCA process for identifying copyright violators is a threat to privacy or safety. Should that change, however, it would be possible to alter the system in a way that gives a warning letter to a violator before turning over the identifying information to the rights holder; such a system would be an effective "scared straight" tool without infringing privacy.

⁵⁵ <http://edition.cnn.com/interactive/entertainment/0101/cd.price/frameset.exclude.html>.

⁵⁶ For further discussion of these cases, see "Revenge of the Disintermediated: How the Middleman is Fighting E-Commerce and Hurting Consumers," by Robert D. Atkinson, *Progressive Policy Institute*, January 2001, <http://www.ppionline.org>.

⁵⁷ "Bill of Rights," *DigitalConsumer*, <http://www.digitalconsumer.org/bill.html>.

⁵⁸ H.R. 1066 in the 108th Congress. Lofgren's bill would also limit the effectiveness of non-negotiable license agreements that contradict the terms of the Act.

⁵⁹ S. 692 in the 108th Congress.

⁶⁰ These single portal content libraries can be enhanced by metadata tags that add information about the content (artist, title, liner notes, etc.) in a standardized format. This metadata scheme is explained at length in *Customer Driven IT: How Users are Shaping Technology Industry Growth*, by David Moschella, *Harvard Business School Press*, 2003.

⁶¹ Atkinson, Robert D., "The Revenge of the Disintermediated," *Progressive Policy Institute*, January 2001, <http://www.ppionline.org>.

⁶² That is not to say that consumers are completely price insensitive when purchasing content; Madonna's fans might well turn to other artists if her music cost several times more than the average. In general, however, the content industries have priced their products within a narrow band, which has led to low substitutability.

⁶³ Once such case was the lawsuit (later withdrawn) by the National Association of Recording Merchandisers against Sony. The music store trade group sued Sony for placing hyperlinks and materials promoting Sony's direct distribution outlets. "Retailers Sue Sony," *Reuters*, January 31, 2000, <http://www.wired.com/news/business/0,1367,34004,00.html>.

⁶⁴ In "Revenge of the Disintermediated," PPI called for the FTC and DOJ to create "safety zones" that allow for exactly this kind of collaboration, even in all market participants are involved, with the caveat that a formal permission process might be in order. Atkinson, Robert D., "The Revenge of the Disintermediated," *Progressive Policy Institute*, January 2001, <http://www.ppionline.org>.

About the Authors

Shane Ham is the senior policy analyst for PPI's Technology and New Economy Project. He has written on a number of technology-related topics including privacy, spam, domestic defense, global e-commerce, intellectual property, science policy, and government reform.

Prior to joining the Progressive Policy Institute, Mr. Ham served as a writer and producer on a syndicated political talk show, where his assignments focused on the political implications of technology issues. Mr. Ham also worked for the Congressional information division of Lexis-Nexis, where he helped develop and streamline their processes for the collection and dissemination of legislative information. Mr. Ham has been involved with two Internet startup companies. He served as associate editor of *Journal X*, a webzine targeted at young adults with content focused on politics, culture, and technology. He also served on the board of directors for *Gamexpress.com*, an online retailer of high-end board games and video games.

Robert D. Atkinson is the vice president of the Progressive Policy Institute and director of PPI's Technology & New Economy Project. He is the author of the *New Economy Index* series which looks at the impact of the New Economy on the U.S., state, and metropolitan economies. While at PPI, he has written groundbreaking reports on a wide range of technology issues, including the role of IT in homeland defense; Internet taxation, privacy, and spam; global e-commerce; digital government; and middleman opposition to e-commerce. He also directed PPI's New Economy Task Force, co-chaired by Senate Democratic Leader Tom Daschle and Gateway CEO Ted Waitt.

Previously, Dr. Atkinson served as executive director of the Rhode Island Economic Policy Council, a public-private partnership including as members the governor, legislative leaders, and corporate and labor leaders. Prior to that, he was project director at the former Congressional Office of Technology Assessment. While at OTA, he directed *The Technological Reshaping of Metropolitan America*, a report examining the impact of the information technology revolution on America's urban areas. He is a board member of the NanoBusiness Alliance and the Information Policy Institute, and was appointed by President Clinton to the Commission on Workers, Communities, and Economic Change in the New Economy. He is also a member of the Task Force on National Security in the Information Age, co-chaired by Markle Foundation president Zoe Baird and former Netscape Communications chairman James Barksdale. In 2002, *Government Technology* magazine and the Center for Digital Government named him one of the 25 top "Doers, Dreamers and Drivers of Information Technology."