Better to be conservative and not introduce products with features that might prompt a lawsuit, even if you are reasonably sure that your products are legal.

We can speculate about products and features that are unavailable today due to the uncertainties in *Grokster's* "intent" standard, coupled with penalties for secondary infringement penalties that could lead to nightmarish fines. Companies are naturally reluctant to give examples, but one might ask why songs shared wirelessly with Microsoft Zune players self-destruct after three plays, or why Tivo recorders don't have automatic commercial skipping or let you move recorded movies to a PC. Non-coincidentally, in 2002, the CEO of a major cable network characterized skipping commercials while watching TV as theft, although he allowed that "I guess there could be a certain amount of tolerance for going to the bathroom."

But speculating about the consequences of liability alone is largely pointless, because these liability risks have not been increasing in a vacuum. A second front has opened up in the copyright wars. Here, the weapons are not lawsuits, but technology.

Authorized Use Only

Computers process information by copying bits—between disk and memory, between memory and networks, from one part of memory to another. Actually, most computers are able to "keep" bits in memory only by recopying them over and over, thousands of times a second. (Ordinary computers use what is called Dynamic Random Access Memory, or DRAM. The copying is what makes it "dynamic.") The relation of all this essential copying to the kind of copying governed by copyright law has been intellectual fodder for legal scholars—and for lawyers looking for new grounds on which to sue.

Computers cannot run programs stored on disk without copying the program code to memory. The copyright law explicitly permits this copying for the purpose of running the program. But suppose someone wants simply to *look at* the code in memory, not to run it. Does that require explicit permission from the copyright holder? In 1993, a U.S. Federal Circuit Court ruled that it does.

Going further, computers cannot display images on the screen without copying them to a special part of memory called a display buffer. Does this mean that, even if you purchase a computer graphic image, you can't view the image without explicit permission from the copyright holder each time? A 1995 report from the Department of Commerce argued that it does mean exactly this, and went on to imply that almost any use of a digital work involves making a copy and therefore requires explicit permission.

Digital Rights and Trusted Systems

Legal scholars can debate whether copyright law mandates a future of "authorized use only" for digital information. The answer may not matter much, because that future is coming to pass through the technologies of digital rights management and trusted systems.

The core idea is straightforward. If computers are making it easy to copy and distribute information without permission, then *change computers* so that copying or distributing without permission is difficult or impossible. This is not an easy change to make; perhaps it cannot be done at all without sacrificing the computer's ability to function as a general-purpose device. But it's a change that's underway nonetheless.

Here is the issue: Suppose (fictitious) Fortress Publishers is in the business of selling content over the Web. They'd like the only people getting their content to be those whose pay. Fortress can start by restricting access on their web site to registered users only, by requiring passwords. Much web content is sold like this today—for instance, *Wall Street Digest* or *Safari Books Online*. The method works well (or at least has worked well so far) for this type of material, but there's a problem with higher-value content. How does Fortress prevent people who've bought its material from copying and redistributing it?

One thing Fortress can do is to distribute their material in encrypted form, in such a way that it can be decrypted and processed only by programs that obey certain rules. For instance, if Fortress distributes PDF documents created with Adobe Acrobat, it can use Adobe LiveCycle Enterprise Suite to control whether people reading the PDF file with Adobe Reader are allowed to print it, modify it, or copy portions of it. Fortress can even arrange to make a document "phone home" over the Internet—i.e., to notify Fortress whenever it is opened and report the IP address of the computer that is opening it. Similarly, if Fortress prepares music files for use with Windows Media Player, it can use Microsoft Windows Media Rights Manager to limit the number of times the music can be played, to control whether it can be copied to a portable player or a CD, force it to expire after a certain period of time, or make it phone home for permission each time it's played so that the Fortress web server can check a license and require payment if necessary.

The general technique of distributing content together with control information that restricts its use is called *digital rights management* (DRM). DRM systems are widely used today, and there are industry specifications (called *rights expression languages*) that detail a wide range of restrictions that can be imposed.

DRM might appear to solve Fortress's problem, but the approach is far from airtight. How can Fortress be confident that people using their material are

using it with the intended programs, the ones that obey the DRM restrictions? Encrypting the files helps, but as explained in Chapter 5, attackers break that kind of encryption all the time—it happens regularly with PDF and Windows Media. More simply, someone could modify the document reader or the media player program to save unencrypted copies of the material as they are running, and then distribute those copies all over the Internet for anyone's use.

To prevent this, Fortress could rely on the computer operating system to require that any program manipulating their content must be certified. Before a program is run, the operating system checks a digital signature for the program to verify that the program is approved and has not been altered. That's better, but a really clever attacker might alter the operating system so that it will run the modified program anyway. How could anyone prevent that? The answer is to build a chip into every computer that checks the operating system each time the machine is turned on. If the operating system has been modified, the computer will not boot. The chip should be tamper-proof so that any attempt to disable it will render the machine inoperable.

Encryption and DRM

Chapter 5 explains public-key encryption and digital signatures—the technologies that make public distribution of encrypted material possible. The "messages" that Alice and Bob are exchanging might be not text messages, but rather music, videos, illustrated documents, or anything at all. As the first koan says, "it's all just bits." Thus, the encryption technologies that Alice and Bob use for secret communication can be used by content suppliers to control the conditions under which consumers can watch movies or listen to songs.

This basic technique was worked out during the 1980s and demonstrated in several research and advanced development projects, but only since 2006 has it been ready for wide deployment in consumer-grade computers. The required chip, called a *Trusted Platform Module* (TPM), was designed by the *Trusted Computing Group*, a consortium of hardware and software companies formed in 1999. More than half of the computers shipped worldwide today contain TPMs. Popular operating systems, including Microsoft Windows Vista and several versions of GNU/Linux, can use them for security applications. One application, *trusted boot*, prevents the computer from booting if the operating system has been modified (for example, by a virus). Another application, called *sealed storage*, lets you encrypt files in such a way that they can be decrypted only on particular computers that you specify. Given today's concerns over viruses and Internet security, it's a safe bet that TPMs will become pervasive. One industry estimate shows that more than 80% of laptop PCs will include TPMs by 2009.

Asserting Control Beyond the Bounds of Copyright

Fortress Publishers' problem could be solved in a world of digital rights management reinforced by trusted computing, but is that something we should welcome?

For one thing, it gives Fortress a level of control over use of its material that goes far beyond the bounds of copyright law. When we buy a book today, we take for granted that we have the right to read it whenever we like and as many times as we like; read it from cover to cover or skip around; lend it to a friend; resell it; copy out a paragraph for use in a book report; donate it to a school library; open it without "phoning home" to tell Fortress we are doing so. We need no permission to do any of these things. Are we willing to give up these rights when books are digital computer files? How about music? Videos? Software? Should we care?

Now leave to one side, for a moment, the dispute between music companies and listeners. DRM and trusted computing technologies, once standard in personal computers, will have other uses. The same methods that, in one country, prohibit people from playing unlicensed songs can, in another country, prevent people from listening to unapproved political speeches or reading unapproved newspapers. Developers of DRM and trusted platforms may be creating effective technologies to control the use of information, but no one has yet devised effective methods to circumscribe the limits of that control. As one security researcher warned: "Trusted computing" means that "third parties can trust that your computer will disobey your wishes."

The same methods that, in one country, prohibit people from playing unlicensed songs can, in another country, prevent people from listening to unapproved political speeches or reading unapproved newspapers.

Another concern with DRM is that it increases opportunities for technology lock-in and anticompetitive mischief. It is tempting to design operating systems that run only certified applications in order to protect against viruses or bogus document readers and media players. But this can easily turn into an environment where no one can market a new media player without publishers' approval, or where no one can deploy *any* application without first having it registered and approved by Microsoft, HP, or IBM. A software company that poses a competitive threat to established interests, like publishers, operating system vendors, or computer manufacturers, might suddenly encounter "complications" in getting its products certified. One reason innovation has been so rapid in information technology is that the infrastructure is open: You don't need permission to

introduce new programs and devices on the Internet. A world of trusted systems could easily jeopardize this.

A third DRM difficulty is that, in the name of security and virus protection, we could easily slip into an unwinnable arms race of increasing technology lock-down that provides no real gain for content owners. As soon as attackers anywhere bypass the DRM to produce an unencrypted copy, they can distribute it—and they might be willing to go to a lot of effort to be able to do that.

Think, for example, about making unauthorized copies of movies. Very sophisticated attackers might modify the TPM hardware on their computers, putting a lot of effort into bypassing the tamper-proof chip. Here's an even easier method: let the TPM system operate normally, but hook up a video recorder in place of the computer display. That particular attack has been anticipated by the industry with a standard that requires all high-definition video to be transmitted between devices in encrypted form. Windows Vista implements this in its *Output Protection Management* subsystem, out of concern that otherwise the movie studios would not permit high-definition video to be played on PCs at all. Even that protection scheme is vulnerable—you could simply point a video recorder at the screen. The result would not be high-definition quality, but once it has been digitized, it could be sent around the Internet without any further degradation.

Content owners worried about these sorts of attacks refer to them as the *analog hole*, and there seems to be no technological way to prevent them. J.K. Rowling tried to prevent unauthorized Internet copies of *Harry Potter and the Deathly Hallows* by not releasing an electronic version of the book at all. That did not stop the zealous fan mentioned in Chapter 2 from simply photographing every page and posting the entire book on the Web even before it was in bookstores.

In the words of one computer security expert, "Digital files cannot be made uncopyable, any more than water can be made not wet." There is one thing for certain: The DRM approach to copyright control is difficult, frustrating, and potentially fraught with unintended consequences. Out of that frustration has emerged a third response—along with liability and DRM—to the increasing levels of copying on the Internet: outright criminalization of technology.

Forbidden Technology

The lines of text following this paragraph might be illegal to print in a book sold in the United States. We've omitted the middle four lines to protect ourselves and our publisher. Had we left them in, this would be a computer

program, written in the Perl computer language, to unscramble encrypted DVDs. Informing you how to break DVD encryption so you could copy your DVDs would be a violation of 17 USC §1201, the *anti-circumvention* provision of the 1998 Digital Millennium Copyright Act (DMCA). This section of the DMCA outlaws technology for bypassing copyright protection. Don't bother turning to the back of the book for a note telling you where to find the missing four lines. A New York U.S. District Judge ruled in 2000 that even providing so much as a web link to the code was a DMCA violation in itself, and the Appeals Court agreed.

```
s''$/=\\2048;while(<>){G=29;R=142;if((@a=unqT="C*",_)[20]&48){D=89;_unqb24.qT.@

. . . (four lines suppressed) . . .

)+=P+( F&E))for@a[128..$#a]\\}print+qT.@a}';s/[D-HO-U_]/\\$$&/g;s/q/pack+/g;eval
```

The DMCA's anti-circumvention rules do more than stop people from printing gibberish in books. They outlaw a broad class of technologies—outlaw manufacturing them, selling them, writing about them, and even talking about them. That Congress took such a step shows the depth of the alarm and frustration at how easily DRM is bypassed. With §1201, Congress legislated, not against copyright infringement, but against bypassing itself, whether or not anything is copied afterwards. If you find an encrypted web page that contains the raw text of the Bible and break the encryption order to read Genesis, that's not copyright infringement—but it *is* circumvention. Circumvention is its own offense, subject to many of the same penalties as copyright infringement: statutory damages and, in some cases, imprisonment. Congress intentionally chose to make the offense independent of actual infringement. Alternative proposals that would have limited the prohibition to circumvention for the purpose of copyright infringement were considered and defeated.

The DMCA prohibition goes further. As §1201(a)(2) decrees:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that ... is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [copyright].

Here the law passes from regulating behavior (circumvention) to regulating technology itself. It's a big step, but in the words of one of the bill's

supporters at the time, "I continue to believe that we must ban devices whose major purpose is circumvention because I do not think it will work from the enforcement standpoint. That is, allowing anti-circumvention devices to proliferate freely, and outlaw only the inappropriate use of them, seems to me unlikely to deter much."

In the arena of security, there is an odd asymmetry between the world of atoms and the world of bits. There are many published explanations of how to crack mechanical combination locks, and even of how to construct a physical master key for a building from a key to a single lock in the set. But if the lock is digital, and what is behind it is *Pirates of the Caribbean*, the rules are different. Federal law prohibits publication of any explanation of how to reverse-engineer that kind of lock.

Legislators may not have seen an effective alternative, but they crafted an awkward form of regulation that begins with a broad prohibition and then grants exemptions on a case-by-case basis. The need for exemptions became apparent even as the DMCA was being drafted. A few exemptions got written into the statute. These included permission for intelligence and law enforcement agents to break encryption during the course of investigations and permission for non-profit libraries to break the encryption on a work, but only for the purpose of deciding whether to buy it. The law also included a complex rule that allows certain types of encryption research under certain circumstances. Recognizing that needs for new exemptions would continue to arise, Congress charged the Librarian of Congress to conduct hearings to review the exemptions every three years and grant new ones if appropriate.

For instance, in November 2006, after a year-long hearing process, a new exemption gave Americans the right to undo the lock-in on their mobile phones for the purpose of shifting to a new cellular service provider. The ruling had a big impact nine months later in August 2007, when Apple released its iPhone, locked to the AT&T cellular network. Users clamored to unlock their iPhones so they could be used on other networks, and several companies began selling unlocking services. But the language of the DMCA and the exemption is so murky that, while unlocking your *own* phone is legal, distributing unlocking software or even *telling* other people how to unlock their phones might still be a DMCA violation. Indeed, AT&T threatened legal action against at least one unlocking company.

Copyright Protection or Competition Avoidance?

The DMCA's framework for regulation is a poor match to technology innovation, because the lack of an appropriate exemption can stymie the deployment of a new device or a new application. Given the ferocity of industry

competition, there's the constant temptation to exploit the broad language of the prohibition as grounds for lawsuits against competitors.

In 2002, the Chamberlain garage-door company sued a maker of universal electronic garage-door openers, claiming that the universal transmitters circumvented access controls when they sent radio signals to open and close the doors. It took two years for the case to finally die at the appeals court. That same year, Lexmark International sued a company that made replacement toner cartridges for Lexmark printers, charging that the cartridges circumvented access controls in order to function with the printer. The District Court agreed. The ruling was overturned on appeal in 2004, but in the meantime, the alternative cartridges were kept off the market for a year and a half. In 2004, the Storage Technology Corporation successfully convinced the Boston District Court that it was a DMCA violation for third-party vendors to service its systems. Had the appeals court not overturned the ruling, we might now be in a situation where no independent company could service computer hardware. It would be as if Ford Tauruses came with their hoods sealed, and it was illegal for any mechanic not licensed by Ford to service them.

Lawsuits like these earned the DMCA the epithet "Digital Millennium Competition Avoidance." Fortunately, none of the lawsuits were ultimately successful, because the courts ruled that the underlying disputes weren't sufficiently related to copyrighted material—it's unlikely that Congress intended the DMCA to apply to garage doors. But in areas where copyright enters, the anti-competitive impact of the DMCA emerges in full force.

Imagine that the 1984 Supreme Court ruling in the *Sony* case had gone the other way, and the Court had declared Sony liable for copyright infringement for selling VCRs. Would VCRs have disappeared? Almost certainly not—consumers wanted them. More likely, the electronics industry would have cut a deal with the motion picture industry, giving them control over the capabilities of VCRs. VCRs would have become highly regulated machines, regulated to meet the demands of the motion picture industry. All new VCR features would need to be approved, and any feature the MPAA didn't like would be kept off the market. The capabilities of the VCR would be under the control of the content industry.

That's the kind of world we are living in today when it comes to digital media. If a company manufactures a product that processes digital information, it needs to be concerned about copyright infringement, even without the DMCA. This is a big concern, especially after *Grokster*. But suppose the device could not be used for copyright infringement. Even then, if the digital information is restricted by DRM, the product must abide by the terms of the DRM restrictions. Otherwise, that would be circumvention, so the product couldn't be legally manufactured at all. The terms of the DRM restrictions

are completely at the whim of the content provider. Once Fortress Publishers installs DRM, they get to dictate the behavior of any device that accesses their material.

In the case of DVDs, DVD content is encrypted with an algorithm called the Content Scrambling System (CSS), developed by Matsushita and Toshiba and first introduced in 1996. As mentioned in Chapter 5, that algorithm was quickly broken—a textbook violation of Kerckhoffs's Principle—and underground decryption programs are today readily found on the Internet. The censored six lines of text earlier in this chapter is one such program.

Although CSS is useless for realistic copy protection, it is invaluable as an enabler of anti-competitive technology regulation. Any company marketing a product that decrypts DVDs needs a license from the DVD Copy Control Association (DVD CCA), an organization formed in 1999. The license conditions are determined by whatever the CCA decides. For example, all DVD players must obey "region coding," which limits them to playing DVDs made for one part of the world only, and an individual player's region can be changed no more than five times. Region coding has nothing to do with copyright. It is there to support a motion picture industry marketing strategy of releasing movies in different parts of the world at different times. The varied license restrictions include some that companies are not even permitted to see until after they have signed the license.

The Face of Technology Lock-in

Suppose you are a company with an idea for an innovative DVD product. Maybe it is a home entertainment system that lets people copy and store DVDs for later watching, and you have worked out a way to do this without encouraging copyright infringement. This is an actual product. Kaleidescape, the California start-up that makes it, was sued by the DVD CCA in 2004 for violating a provision of the CSS license that forces DVD players to be designed to work only when there is a physical disk present. In March 2007, a California court ruled in Kaleidescape's favor, on the grounds that the license wasn't clear enough, but the case is being appealed. In any case, the CCA can change the license at any time. The legal wrangling has kept the company under a cloud for three years. Another start-up working on a similar product at the same time folded when it failed to get venture funding, "in part due to the threat of legal action from the DVD CCA."

The DVD technology lock-in has been in place since 2000. A similar lock-in is being implemented for high-definition cable TV. A campaign to extend the lock-in to all consumer media technology is being promoted in Washington as the *broadcast flag initiative*. And more trial balloons keep

being floated in the name of protecting copyright. A bill was introduced in Congress to ban home recording of satellite radio. NBC urged the Federal Communications Commission to force Internet service providers to filter all Internet traffic for copyright infringement (that is, to compel ISPs to check packets as they are passed around the Internet and to discard packets deemed to contain unauthorized material). In 2002, Congress considered a breathtakingly broad prohibition against *any* communications device that does not implement copyright control—a bill that had to be redrafted after it became apparent that the first draft would have banned heart pacemakers and hearing aids.

So, in the United States today, a technology company is free to invent a new garage-door opener without needing its design approved by the garage-door makers. It can manufacture cheaper replacement toner cartridges without approval from the printer companies. It cannot, however, create new software applications that manipulate video from Hollywood movie DVDs without permission from the DVD CCA. It cannot in principle create *any* new product or service around DRM-restricted digital content without getting permission, often from the very people who might regard that new product as a competitive threat.

This is the regulatory posture at the present juncture in the copyright wars. People can debate the merits of this position. Some say that the DMCA is necessary. Others claim that it has been largely ineffective in curtailing infringement, as the continuing calls for ever more severe copyright penalties demonstrate. But whatever its merits, the anti-circumvention approach is poisonous to the innovation that drives the digital age. It hobbles the rapid deployment of new products and services that interoperate with existing infrastructure. The uncertain legal risks drive away the venture capital needed to bring innovations to market.

The anti-circumvention approach is poisonous to the innovation that drives the digital age.

In essence, the DMCA has enlisted the force of criminal law in the service of the lock-in shenanigans invited by DRM. It has introduced anti-competitive regulation under the guise of copyright protection. By outlawing technology for circumventing DRM, the law has, in the words of one critic, become a tool for "circumventing competition."

Public Knowledge (`publicknowledge.org`) is a Washington DC public-interest group that focuses on policy issues concerning digital information. See their "issues" and "policy" blogs to stay current on the latest happenings in Washington.

Copyright Koyaanisqatsi: Life Out of Balance

1982 marked the release of an astonishing film called *Koyaanisqatsi*. The title is a Hopi Indian word meaning "life out of balance." The film, which has no dialogue or narration, barrages viewers with images at once hauntingly beautiful and deeply disturbing, images that juxtapose the world of nature with the world of cities. The relentless message is that technology is destroying our ability to live harmonious, balanced lives.

In the first decade of the twenty-first century, we inhabit a world of copyright koyaanisqatsi. Virtually every salvo in the copyright war, Congressional bill introduced, lawsuit filed, court ruling issued, or advocacy piece trumpeted, pays homage to the "traditional balance of copyright" and the need to preserve it. The truth is that the balance is gone, toppled in the digital explosion, which is likewise shattering the framework for any civil consensus over the disposition of information. The balance is gone for good reason.

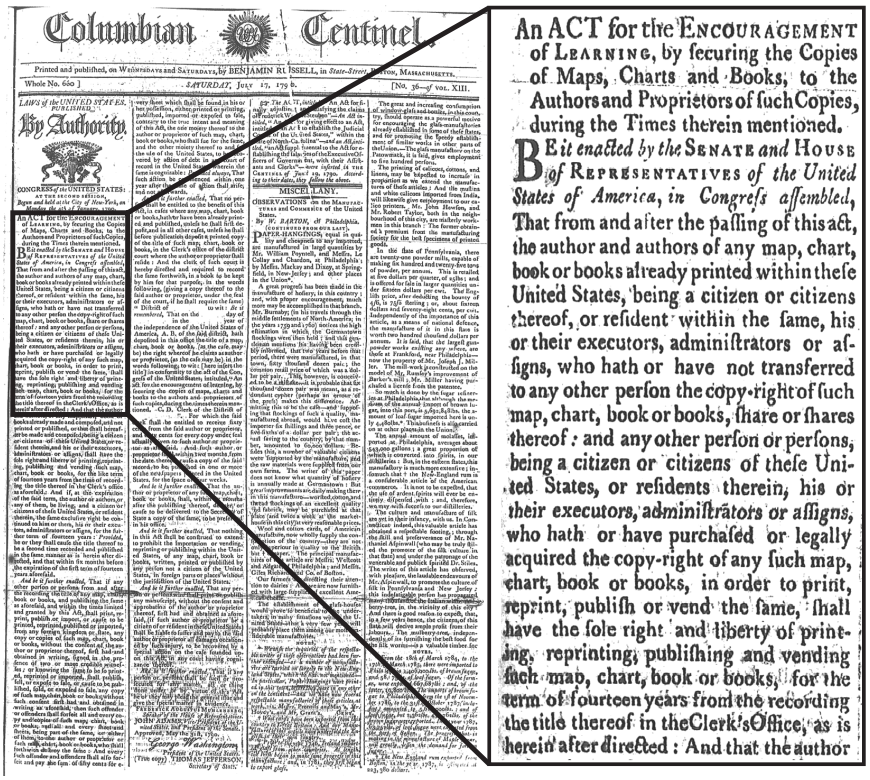
Copyright (at least in the United States) is supposedly a deal the government strikes between the creator of a work and the public. The creator gets limited monopoly control over the work, for limited times, which provides the opportunity to benefit commercially. The public gets the benefit of having the work, and also gets to use it without restriction after the monopoly has expired. The parameters of the deal have evolved over the years, generally in the direction of a stronger monopoly. Under the first U.S. copyright law, enacted in 1790, copyright lasted a maximum of 28 years. Today, it lasts until 70 years after the author's death. In principle, however, it's still a deal.

It is an enormously complex deal, and it is easy see why. Today's copyright law is the outcome of 200 years of wrangling, negotiating, and compromising. The first copyright statute was printed in its entirety in two newspaper columns of the *Columbian Centinel*, shown in Figure 6.3. As the enlarged text insert shows, the law covered only maps, charts, and books, and granted exclusive rights to "print, reprint, publish, or vend." The period of copyright was 14 years (with a 14-year renewal). Today's statute runs to more than 200 pages. It's a Byzantine stew peppered with exceptions, qualifications, and arcane provisions. You can't make a public performance of a musical work unless you're an

DIGITAL COPYRIGHT

Digital Copyright by Jessica Litman (Prometheus Books, 2001) recounts the evolution of U.S. copyright law as a series of negotiated compromises. The Citizen Media Law Project (`www.citmedialaw.org`) offers useful information to online publishers—not just about copyright, but other legal matters as well.

agricultural society at an agricultural fair. You can't freely copy written works, but you can if you're an association for the blind and you're making an edition of the work in Braille (but not if the work is a standardized test). A radio station can't broadcast a recording without a license from the music publisher, but it doesn't need a license from the record company—but that's only if it's an analog broadcast. For digital satellite radio, you need licenses from both (but there are exceptions).



Columbian Centinel

Printed and published, on Wednesdays and Saturdays, by BENJAMIN RUSSELL, in State-Street, Boston, Massachusetts.

Whole No. 660] SATURDAY, July 17, 1790. [No. 36—of vol. XIII.

LAWS of the UNITED STATES, PUBLISHED By Authority.

CONGRESS of the UNITED STATES: AT THE SECOND SESSION, Begun and held at the City of New-York, on Monday the 4th of January, 1790.

AN ACT for the ENCOURAGEMENT of LEARNING, by securing the Copies of Maps, Charts and Books, to the Authors and Proprietors of such Copies, during the Times therein mentioned.

BE it enacted by the SENATE and HOUSE of REPRESENTATIVES of the United States of America, in Congress assembled, That from and after the passing of this act, the author and authors of any map, chart, book or books already printed within these United States, being a citizen or citizens thereof, or resident within the same, his or their executors, administrators or assigns, who hath or have not transferred to any other person the copy-right of such map, chart, book or books, share or shares thereof: and any other person or persons, being a citizen or citizens of these United States, or residents therein, his or their executors, administrators or assigns, who hath or have purchased or legally acquired the copy-right of any such map, chart, book or books, in order to print, reprint, publish or vend the same, shall have the sole right and liberty of printing, reprinting, publishing and vending such map, chart, book or books, for the term of fourteen years from the recording the title thereof in the Clerk's Office, as is herein after directed: And that the author

Harvard University Library.

FIGURE 6.3 The first U.S. copyright law—"An Act for the Encouragement of Learning." It was printed as the first two columns of the July 17, 1790 edition of the *Columbian Centinel*. Note George Washington's signature on the bill at the bottom of the second column.

It is a law written for specialists, not for ordinary people. Even ordinary lawyers have trouble interpreting it. But that never mattered, because the copyright deal never was about ordinary people. The so-called "copyright balance" was largely a balancing act among competing business interests. The

evolution of copyright law has been a story of the relevant players sitting down at the table and working things out, with Congress generally following suit. Ordinary people were not involved, because ordinary people had no real ability to publish, and they had nothing to bring to the table.

Late to the Table

The digital explosion has changed all that by making it easy for anyone to copy and distribute information on a world-wide scale. We can all be publishers now. The public is now a party to the copyright deal—but the game has been going on for 200 years, and the hands were dealt long ago.

When people come to the table with their new publishing power, expecting to take full advantage of information technology, they find that there are possibilities that seem attractive, easy, and natural, but for which the public's rights have already been "balanced" away. Among the lost opportunities are copying a DVD to a portable player, making the video clip equivalent of an audio mixtape, placing a favorite cartoon or a favorite song on a Facebook page, or adding your own creative input to a work of art you love and sharing that with the world.

People resent it when acts like these are denounced as theft and piracy. As a contributor to a computer bulletin board quipped, "My first-grade teacher told me I should share, and now they're telling me it's illegal."

Can You Copy Music CDs to Your Computer?

Of course, you *can* easily copy CDs to your computer hard drive: There are dozens of software packages designed to do just that, and millions of people do it regularly. Yet the legal issues in CD copying are both murky and confusing—a striking example of the mismatch of copyright law and public understanding.

In testimony at the Jammie Thomas trial in October 2007 (see the sidebar earlier this chapter), Jennifer Pariser, the head of litigation for Sony BMG, suggested that ripping your own legally purchased CD, even for personal use, is illegal, asserting that making a copy of a purchased song is just "a nice way of saying 'steals just one copy'." The RIAA web site specifically states that there is no legal right to copy music CDs, although it allows that copying music "usually won't raise concerns" so long as the copy is for personal use, and it warns that it's illegal to give your copy away or lend it to others to copy.

In contrast, in an October 2006 poll of Los Angeles teenagers, 69% believed that it *is* legal to copy a CD from a friend who had purchased it.

That resentment can easily grow to a sense of moral outrage. In the words of Electronic Frontier Foundation founder, John Gilmore:

> What is wrong is that we have invented the technology to eliminate scarcity, but we are deliberately throwing it away to benefit those who profit from scarcity. We now have the means to duplicate any kind of information that can be compactly represented in digital media.... We should be rejoicing in mutually creating a heaven on earth! Instead, those crabbed souls who make their living from perpetuating scarcity are sneaking around, convincing co-conspirators to chain our cheap duplication technology so that it *won't* make copies—at least not of the kind of goods *they* want to sell us. This is the worst sort of economic protectionism—beggaring your own society for the benefit of an inefficient local industry.

But one person's sharing can be another person's theft, and the other side in the copyright war has no shortage of its own moral outrage. The motion picture industry estimates that the retail value of unauthorized movie copies floating around the Internet is more than $7 billion. As the president of the MPAA puts it:

> We will not welcome ... theft masquerading as technology. No business, including the movies, can keep its doors open, its employees paid, and its customers satisfied if pirates and thieves are allowed to run ramshackle over this country's basic protection of the right of individuals to the ownership of their creative expressions, and to benefit from those expressions and that ownership.

This is not "balance." It's a nasty firefight filled with indignation, recriminations, and a path of escalating punishments and anticompetitive regulation in the name of copyright law. As collateral damage of the battle, innovation is being held hostage.

Toward De-Escalation

Getting off that path requires freeing ourselves of old ideas and perspectives. Difficult as that seems, there are grounds for optimism. During 2007, the recording industry made a major shift away from reliance on digital rights

management. In addition to restraints it imposes on technology, DRM is an inconvenience both for consumers and publishers. There has been an increasing public acknowledgement of the downsides of DRM, not only by consumer groups, but by the industry itself.

One of the first visible moves was an announcement in February 2007 by Apple's Steve Jobs, in the form of an open letter to recording industry executives asking them to relax the licensing restrictions that required Apple to implement DRM on iTunes music. In Jobs's view, a world of online stores selling DRM-free music that could play on any player would be "clearly the best alternative for consumers, and Apple would embrace it in a heartbeat." The industry reacted coldly, but other groups chimed in to agree with Jobs. In March, Musicload, one of Europe's largest online music retailers, came out against DRM, noting that 75% of its customer service calls were due to DRM. Musicload asserted that DRM makes using music difficult for consumers and hinders the development of a mass market for legal downloads. In November, the British Entertainment Retailers Association also came out against DRM. Its director general claimed that copy protection mechanisms were "stifling growth and working against the consumer interest."

By the summer of 2007, Apple iTunes and (separately) Universal Music Group began releasing music tracks that could be freely copied. The iTunes tracks contained information ("watermarks") identifying the original purchaser from iTunes. That way, if large numbers of unauthorized copies would appear on the Internet, the original purchaser could be traced and held accountable.

A few months later, even that level of restriction was vanishing. By the beginning of 2008, all four major music labels—Universal, EMI, Warner, and Sony/BMG—were releasing music for sale through Amazon without watermarks that identified individual buyers. It was a remarkable about-face over the course of a year. When Jobs made his February 2007 proposal, Warner Music CEO Edgar Bronfman flat-out rejected the idea as "completely without logic or merit." Before the end of the year, Warner was announcing that it would

Using Watermarking

Using watermarking rather than copy restrictions and access control is an example of a general approach to regulation through *accountability*, rather than *restriction*. Don't try to prohibit violations in advance, but make it possible to identify violations when they occur and deal with them then. The same perspective can apply in privacy, as mentioned in Chapter 2, where one can focus on the appropriate use of personal information rather than restricting access to it.

sell DRM-free music on Amazon, with Bronfman explaining in a note to employees:

> By removing a barrier to the sale and enjoyment of audio downloads, we bring an energy-sapping debate to a close and allow ourselves to refocus on opportunities and products that will benefit not only WMG, but our artists and our consumers as well.

The increasing recognition that the DRM approach is failing is sparking experiments with other models for distributing music on the Internet. Universal has been talking to Sony and other labels about a subscription service, where users would pay a fixed fee and then get as much music as they want. One plan links the service to a new hardware device, here the price of the service would be folded into the price of the hardware.

A related idea is to distribute music through blanket licenses with mobile carriers or ISPs. New companies are emerging that offer this kind of service on college computer networks. Another variant is the idea of *unlimited content networks*. These are networks that give access to music or video that floats around the network with no restrictions. People can make unlimited use of the material—downloading, copying, moving it to portable devices, sharing with others—as long as they keep it within the network.

A complementary approach promotes sharing of music and other creative works in a way that enriches the common culture, by making it easy for creators to distribute their own work and to build on each other's work. One organization that provides technical and legal tools to encourage this is *Creative Commons*. This organization distributes a family of copyright licenses that creators can use for publishing their works on the Internet, including licenses that permit open sharing. The licenses are expressed both as legal documents and as computer code that can support new applications. If a work appears on the Web with the appropriate Creative Commons code, for example, search engines might return references to it when asked to find material that can be used under specified licensing conditions. Stimulating open sharing on the Internet is an example of moving toward a *commons*—that is, a system of sharing that minimizes the need for fine-grained property restrictions (Chapter 8, "Bits in the Air" includes more on the notion of a commons).

Experience with these and other approaches will show whether there are economically viable models for distributing music that do not rely upon

DRM. Success could pave the way for the motion picture industry and other publishers to get off the anti-circumvention path—a dead end that has been more effective at harming innovation than at stopping infringement, and which even some of the original architects of the policy are now acknowledging as a failed approach.

CREATIVE COMMONS LICENSES

If you've created works that you want to publish on the Internet, you can use the Creative Commons license generator at `creativecommons.org` to obtain a license tailored to your needs. With the license, you can retain specified rights of your choice while granting blanket permission for other uses.

Even then, however, the larger problems created by the DMCA would not fade away, since policies locked into law are not easily unlocked. If the content industry moves to better business models and the DRM battles subside, the DMCA's anticircumvention provisions may continue to be anti-consumer, anti-competitive blots on the digital landscape. Unless repealed from the legal code, they would remain as battlefield relics of a war that was settled by peaceful means—unexploded ordnance that a litigious business could still use in ways unrelated to the law's original intent.

The Limits of Property

For 15 years, the fights over digital music and digital video have been the front line of the copyright wars. Perhaps innovations and experiments that are already underway will help defuse those battles. The enormous potential of the Internet for good—and for profit—need not be sacrificed to combat its abuse. If you do not like what others are doing with the Internet, the Internet does not have to become your enemy—unless you make it your enemy.

The indignation over copyright is intense. The interest in new approaches, such as accountability and commons, suggests the deeper source of the discomfort with the metaphors of property and theft when applied to words and music. The copyright balance that is being toppled by digitization is not just the traditional tension between creator and the public. It is the balance between the individual and society that underlies our notions of property itself. Accountability and commons are attempts to find substitutes for the ever-expanding property restrictions imposed in the name of digital copyright law.

FREE CULTURE

Lawrence Lessig's *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (Penguin, 2004) compellingly traces the story of how overbroad copyright restrictions are jeopardizing the future of a robust and vibrant public culture.

When we characterize movies, songs, and books as "property," we evoke visceral metaphors of freedom and independence: "my parcel of land versus your parcel of land." But the digital explosion is fracturing these property metaphors. "My parcel of land" might be different from "your parcel of land," but when both parcels are blown to clouds of bits, the clouds swirl together. The property lines that would separate them vanish in a fog of network packets.

Learning To Fly Through the Digital Clouds

In 2004, Google embarked on a project, mentioned in Chapter 4, to index the book collections of several large libraries for Google's search engine. The idea is that when you search on the Web, you'll be able to find books relevant to your search query, together with a snippet of text from the book. As Google describes it, they are creating "an enhanced card catalog of the world's books," and this should be no more controversial than any card catalog.

The Association of American Publishers (AAP) and the Authors' Guild object to the Google book project, and they are suing Google for copyright infringement. In the words of the AAP President Patricia Schroeder, "Google is seeking to make millions of dollars by freeloading on the talent and property of authors and publishers." The president of the Authors' Guild equates including a book in the project with stealing the work. At issue is the fact that Google is scanning the books and making copies in order to create the search index, and the case is being debated on legal technicalities about whether this scanning constitutes copyright infringement.

The library project will certainly be beneficial to Google by making its search engine more valuable, and Google is indeed scanning the books without permission from the copyright holders. Are they "appropriating property" and extracting value from it without compensating the owners, not even asking for permission? Should Google be permitted to do that? If you write a book, and that's "property" that you "own," how far should the limits of your ownership extend?

As a society, we have faced this kind of question before. If a stream runs through your land, do you own the water in the stream? Are there limits to your ownership? Can you pump out that water and sell it—even if that would

Copyright and Web Searching

If you believe that the Google library project violates copyright, you might wonder whether search engines themselves infringe copyright by caching and indexing web sites and providing links. This claim has been the source of lawsuits, but the courts have been rejecting it. In *Field v. Google* (January 2006), a Nevada District Court ruled that Google's caching and indexing of web sites is permissible. One of the factors in the ruling was that Google stores web pages in its cache only temporarily. In *Perfect 10 v. Google* (May 2007), the Ninth Circuit Court denied an adult magazine's request for a preliminary injunction to prevent Google from linking to its site and posting thumbnail images from it.

cause water shortages downstream? What about the obligations of landowners upstream from you? These were major controversial issues in the western U.S. in the nineteenth century, which eventually resulted in codifying a system of limited property rights that landowners have to the water running through their land.

Suppose an airplane flies over your land. Is that trespassing? Suppose the plane is flying very low. How far upward does your property right extend? From ancient times, property rights were held to reach upward indefinitely. Perhaps airlines should be required to seek permission from every landowner whose property their planes traverse. Imagine being faced with that regulatory question at the dawn of the Aviation Age. Should we require airlines to obtain that permission out of respect for property and ownership? That might have seemed reasonable at a time when planes flew at only a few thousand feet. But had society done that, what would have been the implications for innovation in air travel? Would we ever have seen the emergence of transcontinental flight, or would the path to that technology have been blocked by thickets of regulation? Congress forestalled the growth of those thickets by nationalizing the navigable airspace in 1926.

Similarly, should we require Google to get permission from every book's copyright holder before including it in the index? It seems perfectly reasonable—and in fact other book indexing projects are underway that do seek that permission. Yet perhaps book search is the fledging digital equivalent of the low-flying aircraft. Can we envision the future transcontinental flights, where books, music, images, and videos are automatically extracted, sampled, mixed, and remixed; fed into massive automated reasoning engines; assimilated into the core software of every personal computer and every cell phone—and thousands of other things for which the words don't even exist yet?

What's the proper balance? How far "upward" into the bursting information space should property rights extend? What should ownership even mean when we're talking about bits? We don't know, and finding answers won't be easy. But somehow, we must learn to fly.

The digital explosion casts information every which way, breaching established boundaries of property. Technologies have confounded copyright—the rules that would regulate and restrain bits in their flight. Technological solutions have been brought to bear on the problems technology created. Those solutions created *de facto* policies of their own, bypassing the considerations of public interest on which copyright was balanced.

Property lines are not the only boundaries the explosion is breaching, and copyright is not the only arena in which information regulation is challenged. Bits fly across national borders. They fly into private homes and public places carrying content that is unwanted, even harmful—content that has historically been restricted, not by copyright, but by regulations against defamation and pornography. Yet the bits fly anyway, and that is the conundrum to which we now turn.