Intellectual Property, Copyright and Digital Rights Management for Computer Graphics

July 2002

Dan L. Burk
University of Minnesota

Barbara Simons
Stanford University

Robert A. Ellis

Course Description

This second course in the policy sequence provides computer graphics practitioners, developers and researchers with an in depth look at the growing conflicts between the rights of owners and users of intellectual property.

The history and legal precedents of copyright will be reviewed and implications of recent treaties and laws such as those developed and administered by the World Intellectual Property Organization (WIPO) and the Digital Millennium Copyright Act (DMCA) in the U.S. will be presented. Implications of digital rights management systems such as the Secure Digital Music Initiative (SDMI), the DVD Content Scrambling System (CSS) and the Content Protection for Recordable Media (CPRM) will be discussed.

Prerequisites

Introduction to Policy Issues in Computer Graphics or equivalent knowledge. We assume a fundamental understanding of public policy, its effect on our professional lives and how it is effected and affected. The material from the introductory course will not be repeated so we can devote adequate time to the material in this course.

Course Syllabus

Copyright Overview (Burk) (10 Minutes)
- U.S. Approach - incentive based
- European Approach - personality based
- International Treaties

Copyright Basics (Burk) (15 Minutes)
- Subject Matter
- Exclusive Rights of Authors
- Fair Use
- Contributory Infringement

Copyright in Digital Media (Burk) (15 Minutes)
- On-line Service Provider (OSP) Liability
- Linking & Framing
- Digital Millennium Copyright Act (DMCA) Anti-circumvention

Digital Rights Management Systems (Simons) (15 Minutes)
- Cryptography
- Watermarking
- Content Scrambling System (CSS)
- Secure Digital Music Initiative (SDMI)
- Content Protection for Recordable Media (CPRM)

Implications of the Use of Digital Rights Management Systems (Simons) (20 Minutes)
- Copyright Owners Have Protection

Fair Use Rights May Be Impacted
Any System Can Be Compromised, Some More Easily Than Others
Works Become Unavailable in the Public Domain and for Archiving

Actions/Discussion (Burk and Simons) (30 Minutes)

Intellectual Property, Copyright and Digital Rights Management for Computer Graphics

July 2002

Dan Burk

Barbara Simons

Bob Ellis

Copyright and Digital Media

Dan L. Burke
University of Minnesota

Copyright © 2002 by Dan L. Burk. Permission to make digital or hard copies of all or part of this work for personal or educational use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page.

Copyright Rationale

- Public Goods Problem
  - non-rival, non-exclusive
  - underproduction
  - incentives
- Trade-off
  - constrained access
  - cost/benefit

Continental Rationale

- Personality Based
  - Autonomy
  - Individuality
- Moral Rights
  - Integrity
  - Attribution

International Framework

- Berne Convention
  - International Minima
- WTO TRIPs
  - International Minima
  - Incorporates Berne
  - WTO Enforcement

Subject Matter

- Originality
  - Authorship
  - Facts, Ideas
- Fixation
  - Tangible Medium
  - Duration

Subject Matter

- Literary Works
- Dramatic Works
- Audiovisual Works
- Sound Recordings
- Musical Compositions
- Pictorial, Graphic, & Sculptural
- Architectural Works

Subject Matter

- Unprotectable
  - Ideas
  - Processes
  - Functional or utilitarian
  - Facts
  - U.S. governmental works

Exclusive Rights

- Reproduction
- Distribution
- Adaptation
- Public Performance
- Public Display
- Digital Transmission

Fair Use

- First Amendment
- Four factors
  - Type of work
  - Amount taken
  - Purpose
  - Impact on market

Contributory Infringement

- Participatory Infringement
  - aiding and abetting
  - knowledge
- Means to Infringe
  - *Sony* standard

DMCA

- Safe Harbors
  - User content
  - Transitory communications
  - Location tools
  - System caching

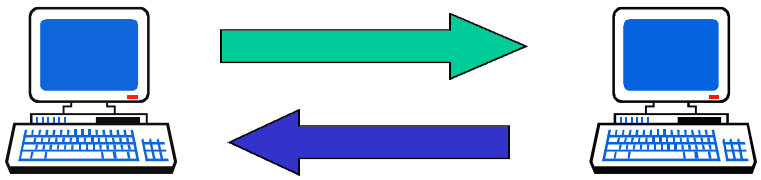
Vicarious Liability

- Agency
  - right to control
  - imputed liability
  - employee
  - agent
- Financial interest

Hypertext Linkage

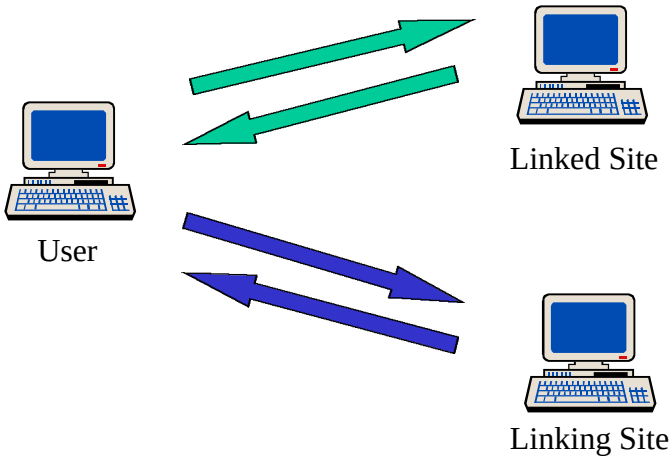
- Direct Infringement
  - Reproduction
  - Distribution
- Contributory Infringement
  - Inducement
  - Vicarious Liability

Universal Resource Locator



DNS lookup

File Retrieval



Direct Infringement

- No reproduction by linking site
- Overlapping uses by linked site
- Authorization
  - Implied license
  - Fair Use

Third Party Liability

- Underlying Direct Infringement
- Contributory Liability
  - Participatory
  - Means to Infringe
- Vicarious Liability

Technological Controls

- Technical Content Management
  - Encryption Software/Hardware
  - Access Control
  - Usage Control
  - Usage Monitoring
  - Payment or Billing
- Conjoined with Licensing

Anti-Circumvention Provisions

- Three Prohibitions
  - Circumventing Access Measures
  - Trafficking in Access Circumvention Tools
  - Trafficking in Usage Circumvention Tools
- Subject to Circumvention Exceptions
  - Governmental Purposes
  - Industry requirements
  - Privacy, possibly fair use

Anti-Circumvention Provisions

- Extremely Broad
  - Regardless of the Nature of the Material
  - Regardless of the User's Motivation
  - Regardless of the Underlying Copyright
- New Form of Intellectual Property
  - "Paracopyright"
- Trafficking Lacks Exemptions

Thank You

Questions Welcome

Implications of Digital Rights Management

Barbara Simons

Copyright © 2001-2002 by Barbara Simons. Permission to make digital or hard copies of all or part of this work for personal or educational use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To otherwise copy, republish, post on servers or redistribute in any manner requires specific prior permission.

"When Congress sits idly by in the face of these activities, we essentially sanction the Internet as a haven for thievery." Sen. Fritz Hollings

"Any attempt to inject a regulatory process into the design of our products will irreparably damage the high-tech industry: it will substantially retard innovation, investment in new technologies, and will reduce the usefulness of our products to consumers." Leslie Vadasz, Executive VP Intel Corp

Senate Commerce Comm. Hearing, Feb. 28, 2002

Copyright

Congress shall have the power ...

To promote the progress of science and the useful arts, by securing for limited times to authors and inventors the exclusive rights to their respective writings and discoveries.

Length of Copyright

- Originally for 14 years
  - renewable for 14 years if author living
- Copyright Act of 1976:
  - retroactively extended to up to 75 years
- Sony Bono Copyright Term Extension Act 1998
  - extended yet another 20 years
  - currently author's life + 70 years
  - "works for hire": the shorter of 95 years from publication or 120 years from creation (MM)

Eldred v. Ashcroft

- Eric Eldred published public domain materials
- Did Congress overstep authority by adding 20 years to length of copyright?
  - Encourages “progress of science and useful arts”?
  - Dead creators?
  - Mickey Mouse

Digital Millenium Copyright Act (DMCA) 1998

- Criminalizes technologies and technological devices
- Selected over alternative (Boucher/Campbell)
- Outlaws reverse engineering, with some exceptions
- Could criminalize some computer security R&D

DMCA: Definitions

- "Technological measure for protecting copyright"?
- "Effectively controls access to a work"?
  - Strong/weak encryption?
  - Data compression?
  - Obscure human language?
  - Compilation? Could decompilation become illegal?
- "Primarily designed" for circumvention?
  - VCRs? Breaking encryption?

DMCA: Criminal Penalties

- Circumvention of "copyright protection" or of "integrity of copyright management information" for commercial advantage or private financial gain:
  - first offense: <= $500K or <= 5 years prison, or both
  - subsequent offenses: <= $1M or <= 10 years prison, or both

Digital Era Copyright Enhancement (Boucher/Campbell)

- Prohibits altering or deleting copyright management information for purposes of infringement
- Prohibits enforcement of terms in "shrink- wrap" and "click-on" agreements when they reduce privileges recognized by copyright law
- Incorporates fair use and first sale rights

Digital Era Copyright Enhancement

- Ensures right of librarians & archivists to preserve copies of copyrighted works using latest technology
- Protects author's work under traditional legal understandings while allowing incidental copies for otherwise lawful use of a device.
- Civil rather than criminal penalties

The DVD Controversy

- DVD movies encrypted using Content Scrambling System (CSS)
  - Weak encryption
- Uses authentication to verify that player or operating system has been licensed
- Who can license open/free software systems?

CSS Broken - DeCSS

- Code broken
  - (Then) 15 year old Jon Johansen or Norwegian group called Masters of Reverse Engineering (MoRE)?
- Subsequently learned that offset provides key with no decryption necessary
- Claim: Need to break CSS in order to run legally purchased DVDs on Linux

Legal Cases Against Posters of DeCSS

- Norway: Jon Johansen
  - Indicted Jan 9, 2002
- New York & Connecticut lawsuits brought by 8 largest movie studios
  - Based on reverse engineering being circumvention of copyright protection
- California case brought by DVD licensing group
  - Trade secret misappropriation - shrink wrap license

DeCSS Legally Available

- DeCSS available in CA case at cryptome.org/dvd-hoy-reply.htm#ExhibitB
- T-shirt with code available at copyleft.net/cgi-bin/copyleft/t039.pl?s1&back
- Dave Touretzky's webpage: http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/
  - haiku, song, steganography, English description, a programming language that has no compiler, ...

MPAA v. Eric Corley A/K/A "Emmanuel Goldstein" and 2600 ENTERPRISES, INC

or

the 2600 DVD Case

Legal Case Against Corley

- Lawsuit brought by Motion Picture Association of America (MPAA)
- Corley accused of posting DeCSS
  - Not accused of deriving DeCSS from CSS
  - Not accused of making illegal copies
- Corley subsequently deleted DeCSS from his web site, and instead posted links to other sites containing DeCSS

Arguments Used by Defense

- Reverse engineering for compatibility allowed under DMCA
- Fair use guaranteed by copyright
  - Should not be able to eliminate indirectly via legislation
  - If DMCA holds, techies who can break encryption will have fair use right, but no one else will … including most judges

Trial Results

- Judge ruled against Corley
  - Enjoined from posting DeCSS
  - Enjoined from **linking** to other sites with DeCSS
  - 2nd U.S. Circuit Court of Appeals upheld lower court ruling
    - Case for defense argued by Kathleen Sullivan, Dean of Stanford Law School

DVDCCA v. Bunner (CA case)

- Nov 1, 2001 CA appeals court overturned an earlier order that barred hundreds of people from publishing the code for DeCSS online. Posting the code is just like publishing other types of controversial speech - protected by Constitution
- programmers could still be prosecuted for posting illegal software but could not be prevented from doing so in the first place.

DVDCCA v. Bunner (CA case)

- “Like the CSS decryption software, DeCSS is a writing composed of computer source code which describes an alternative method of decrypting CSS-encrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS. If the source code were ‘compiled’ to create object code, we would agree that the resulting composition of zeroes and ones would not convey ideas.”

Ed Felten

- Felten and co-authors entered SDMI sponsored contest to defeat watermarking technologies
  - confidentiality agreement prohibiting public discussions of research a precondition for receiving the prize
  - Felten et al did not sign; instead submitted paper to 4th International Information Hiding Workshop

Ed Felten

- Section 1201 of DMCA: “no person shall ... offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that ...” can be used to circumvent “a technological measure that effectively controls access to a [copyrighted] work.”
- Does not address issues such as the robustness of a technological measure or fair use.

Ed Felten

- Two weeks before presentation all authors, all their employers, all program committee members, and all their employers threatened with civil suit by RIAA and SDMI.
  - Withdrew paper
  - Resubmitted to USENIX Conference
    - Brought suit against RIAA, SDMI, Verance, John Ashcroft, and mystery company
  - RIAA, SDMI, Verance promised not to sue

ACM and Felten

- ACM submitted declaration in Felten case
  - Concerned about ACM November '01 Workshop on Security and Privacy in Digital Rights Management
- www.acm.org www.acm.org/usacm/
- Nov 28, 2001 case dismissed by Judge Garrett Brown
  - SDMI, RIAA, and DoJ said they will not sue
  - Felten will not appeal

Dmitry Skylarov

- Arrested for criminal violation of DMCA after presenting paper at DefCon in Las Vegas
  - Russian computer science grad student
  - Talk focused on weaknesses in Adobe copy protection system
  - His company sold software that allowed people who purchased e-books to make copies
    - now available free on the web
  - Allowed to leave US in Dec; agreed to testify later

US v. Elcom Ltd, aka Elcomsoft Co., Ltd, and Dmitry Sklyarov

- EFF amicus signed by USACM, the ACM Law Comm., the American Assoc. of Law Libraries, Music Library Assoc., CPSR, EPIC, CPT, 35 law professors
  - http://www.eff.org/IP/DMCA/US_v_Elcomsoft/

Michael Eisner, CEO of Disney

"[D]igital technologies can enable a level of piracy - theft -that would undermine our capacity to produce films and entertainment, undermine the deployment of Broadband networks, undermine the digital television transition and ultimately result in fewer choices and options for American consumers."

Michael Eisner, CEO of Disney

"[O]nce standards [for digital rights management] are set, they must be mandated for inclusion in all digital media devices that handle creative content. This is necessary to ensure a reasonably secure environment and to prevent unfair competition by non-compliant device manufacturers."

-2/28/02

Proposals to Mandate Copyright Protection

- The Security Systems Standards and Certification Act (SSSCA)
  - circulated, but never introduced by Sen. Hollings
- Consumer Broadband & Digital Television Promotion Act (CBDTPA)
  - introduced March 22, 2002 by Hollings, Feinstein, Stevens, Inouye, Breaux, Nelson
    - 5 Democrats and 1 Republican

SSSCA

- Would have required computer & electronics manufacturers to include copyright-protection technologies in the production of certain products and multi-use devices
  - Sen. Hollings
  - Pushed by Hollywood; opposed by scientific societies, academia, and industry (BSA, etc.)

CBDTPA

- A manufacturer, importer, or seller of digital media devices may not
  - (1) sell, or offer for sale, in interstate commerce, or
  - (2) cause to be transported in, or in a manner affecting, interstate commerce, a digital media device unless the device includes and utilizes standard security technologies that adhere to the security system standards adopted under section 3.

Removal or Alteration of Security Technology (CBDTPA)

- (a) NO person may
  - (1) knowingly remove or alter any standard security technology in a digital media device lawfully transported in interstate commerce; or
  - (2) knowingly transmit or make available to the public any copyrighted material where the security measure associated with a standard security technology has been removed or altered, without the authority of the copyright owner.

Compliance with Encoding Rules (CBDTPA)

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

Digital Media Device (CBDTPA)

- Any hardware or software that
  - (A) reproduces copyrighted works in digital form;
  - (B) converts copyrighted works in digital form into a form whereby the images and sounds are visible or audible; or
  - (C) retrieves or accesses copyrighted works in digital form and transfers or makes available for transfer such works to hardware or software described in subparagraph (B) .

Penalties

- The same as for the DMCA
  - Civil
  - Criminal
    - first offense: <= $500K or <= 5 years prison, or both
    - subsequent offenses: <= $1M or <= 10 years prison, or both

Some Problems

- Research in computer security & protection further curtailed
  - Any such research would be required to be done on (and not interfere with) whatever technology is imposed by this law. However, malicious actors do not need to be so concerned. This has significant national security implications.

Some Problems

- Inclusion of anti-copying technology in general purpose equipment-- real-time computing devices used in traffic control, air flight control, medical equipment, & manufacturing -- adds to their complexity & potential for failure. Unexpected interactions with other code, & accidental activation of protection protocols cannot be ruled out; in many venues the potential for damage is extreme.

Technological Protection for IP

- Technology will solve the problems created by technology => no need for draconian legislation?
  - What if technological “fixes” create as many problems as bad legislation?
    - Will fair use be defined by technology?
    - How will documents be archived?
  - Could device manufacturers be sued for copyright violation?

Why Does Copyright Matter?

- Trade-off: limited time monopoly to encourage creativity and availability of information
- What if information becomes privatized?
  - Education
  - Democracy
  - Science

Where Are We Going?

- What is a library?
- Is copyright being replaced by shrink-wrap licenses?
- Will copyright be replaced by contract law?
- Will we have pay-per-view?
- Do scientists and engineers have any ethical responsibility for how their work is used?

What Can You Do?

- Support professional societies (ACM)
- Interact with policy makers, journalists, other decision makers
- Write or visit your Congressperson

Intellectual Property/Digital Rights Management Tutorial

March 2002
Bob Ellis

We are fortunate to be able to provide, with the permission of the authors and ACM, Inc., a selection of reprints of articles addressing intellectual property as it applies to computing. Although the authors may not be familiar to many SIGGRAPH attendees, they are all recognized experts in their fields.

Copyright for the following articles is held by the authors and/or ACM, Inc. For information contact the individual authors or permissions@acm.org.



PAMELA SAMUELSON,
GUEST EDITOR

INTELLECTUAL PROPERTY FOR AN INFORMATION AGE

How to balance the public interest, traditional legal principles, and the emerging digital reality.

Intellectual property law has suffused the consciousness of computing professionals for the past decade or so. Back in the late 1980s and early 1990s, the "look and feel" lawsuits sent shock waves through the computer-human interaction research and development community. Also hotly debated were questions about whether it was lawful to reverse-engineer another developer's program in order to make a compatible program; whether (or to what extent) the "structure, sequence, and organization" (SSO) of a program was protectable expression under copyright law; and whether algorithms and other program-related innovations could be patented. To aid computing professionals in understanding the legal debates deeply affecting their field, *Communications* began publishing a series of "Legally Speaking" columns to explore these and other controversies and suggest how they might be resolved in a way consistent with traditional principles of the law and with the goal of promoting innovation in the computing field. Now, with this special section on the latest generation of intellectual property issues, *Communications* continues its coverage of this important and contentious aspect of information policy.

The burning issues of a decade ago have subsided. Apple Computer and Lotus Development lost their look and feel cases. Appellate courts in the U.S. and legislatures in other countries decided that reverse engineering software for a legitimate purpose, such as developing an interoperable program, should be lawful as a matter of intellectual property law. While the detailed structure of a program may be eligible for copyright protection—unless it is integral to a process or method of operation—broad SSO claims of the sort that flourished for five years after the infamous

ROBERT NEUBECKER

1986 *Whelan v. Jaslow* decision have died away, as U.S. appellate courts agreed that the *Whelan* decision rested on a flawed understanding of computer science. Meanwhile, patent authorities around the world have become increasingly receptive to claims for computer program-related inventions, including algorithms. On the whole over the past six or seven years, the legal rules on software-protection issues have evolved in a reasonably sound manner.

Computing professionals may well have hoped that once the software intellectual property wars cooled down, they could safely go back to ignoring intellectual property law. However, several recent initiatives having profound implications for the global information environment deserve close attention. The articles in this special section cover five such initiatives likely to have enduring consequences.

Dan L. Burk of the University of Minnesota Law School explores some intriguing and nonobvious implications of the continued expansion of scope of patent protection to cover all manner of information innovations, including free-speech considerations. Randall Davis of MIT unpacks "the digital dilemma" that has led to multiple controversies about digital copyright issues and legislation that has given copyright owners new rights to control piracy-enabling technologies. Yochai Benkler of the New York University School of Law focuses on continuing efforts to enact laws that would create a new form of legal protection for the contents of databases, weighing its implications for an information ecology promoting innovative peer production in the information age. Michael Froomkin of the University of Miami School of Law explains how anticybersquatting law gives trademark owners new rights to control registration of domain names incorporating the marks, along with a new dispute-resolution process the Internet Corporation for Assigned Names and Numbers (ICANN) now requires in every domain name registration contract. And finally, Maureen O'Rourke of the Boston University School of Law chronicles the mushrooming use of the ancient tort of "trespass to chattels" as a way to block unauthorized use of a firm's Web sites and page servers. No one objected in 1996 when AOL got an injunction to stop a commercial spammer from sending email to its customers' accounts by claiming trespass to its servers. More recent cybertrespass cases have created a quasi-intellectual property regime that could radically reshape the entire Internet, including the Web.

Several themes run through these articles. One is the continuing expansion of intellectual property rights, commonly justified on the grounds that this is a necessary response to threats posed by the Internet. Another is a sense of mismatch between traditional legal concepts and emerging digital phenomena. Software may once have seemed the ultimate misfit for intellectual property law; programs are, by nature, both writings and machines, even though the law bifurcates innovations into either writings (assigned to the copyright system) or machines (assigned to the patent system).

Even digitized texts, pictures, and movies now seem mismatched with copyright law, because every access to or every viewing of them inevitably involves making copies. This mismatch between the law and the emerging digital reality in turn means either that rights holders get to control all uses of works, instead of having control over only reproduction and display, or that a new way for distinguishing between acceptable and unacceptable uses has to be developed.

Other misfits with traditional legal principles include proposals to protect the data in databases, new rights to control trademarks embodied in domain names, and virtual trespasses. A larger question underlying these mismatches is whether legal regimes devised for a manufacturing age are well-suited to promote innovation for an information age.

Another theme is how to preserve certain longstanding limiting principles of intellectual property law (such as "fair use" in copyright law) or develop new limiting principles (such as fair use rights for patents) in order to keep an appropriate degree of balance in intellectual property law. If intellectual property rights become too strong, certain industry players may benefit, but such a development would not be good for innovation and consumer welfare in the long run.

Finally, the articles here implicitly seek to at least engage you personally in intellectual property policy in order to ensure that the policymaking process includes all stakeholders, rather than echoing only the voices of intellectual property lobbyists. Sometimes, the additional rights they want may be needed. Sometimes, new rights are needed, though perhaps not as broadly as the lobbyists want. The active input of informed citizens, especially *Communications* readers, can help resolve today's generation of intellectual property issues in a more optimal manner. C

Pamela Samuelson (pam@sims.berkeley.edu) is a professor in the School of Information Management and Systems at the University of California, Berkeley.

© 2001 ACM 0002-0782/01/0200 $5.00

DAN L. BURK

COPYRIGHTABLE FUNCTIONS AND PATENTABLE SPEECH

Defying the legal categories of patent, copyright, and protected speech, and barring a new category all its own, software may be destined for further awkward accommodation in established law.

Computer software is characterized by features that defy classification within established legal doctrines. In particular, areas of the law that rely on distinctions between the "functional" and the "expressive" have found software problematic. In this article, I briefly describe the areas of law in which this problem is most pressing, sketch how these problems have migrated across legal domains, and indicate the path legal controversy attending software seems likely to take, especially in patent law. The picture that emerges is one of continuing legal controversy regarding software within the law of copyright, patent, and free speech, as well as a blurring among these areas as they are stretched to accommodate this chimeric technology.



For more than 20 years, copyright has been the primary mode of intellectual property protection for software in the U.S. and in much of the rest of the world. Copyright covers original works of authorship, including literary works, dramatic works, audiovisual works, musical compositions, audio recordings, pictorial, graphic and sculptural works, choreographic works, and even architectural works. A copyright arises whenever original expression is fixed for some substantial duration in a tangible medium of expression. This act of fixing original expression gives the copyright owner the exclusive right to reproduce and distribute copies of the work, as well as to adapt, publicly

perform, publicly display, and in the case of audio recordings, digitally transmit the work.

The requirement of originality does not mean the work is novel or unprecedented, only that it must originate with the author and is not copied or taken from somewhere else. For this reason, copyright does not extend to facts or mathematical formulae; they are considered to exist in nature, rather than to originate from a human author. Originality also implies a minimum degree of creativity; copyright might cover the selection and arrangement of a compilation of uncopyrightable facts but has been held not to cover a compilation, such as a telephone directory, when the information is predictably arranged in alphabetical order.

Neither does copyright extend to methods, processes, or purely utilitarian items. This rule, now codified in the Copyright Act of 1976 as subsequently amended in 1990, extends back to the 1879 landmark U.S. Supreme Court case of *Baker v. Selden*, in which the plaintiff Selden asserted copyright in printed forms used to practice a method of accounting described in a book he had written on the subject.[1] The Supreme Court reasoned that although Selden could assert copyright in a description of the method, copyright did not extend to the method itself. Anyone else, including the defendant Baker, could legally write his or her own book describing the same method. And since the accounting method could be practiced only by using the forms, the forms were unprotectable as functional items. Protecting the forms under copyright would have been tantamount to protecting the method, and the protection of such items, the Court declared, was the provenance of patent law, rather than of copyright. Absent a patent on the method, Baker could freely use the accounting forms.

The principle of *Baker v. Selden* infuses copyright with a broad antipathy to protection of functional objects. This general principle is explicitly stated in the statute with regard to pictorial, graphic, and sculptural works, which are covered by copyright only as to their separable, nonfunctional characteristics. The specific rule for architectural works is similar, eschewing copyright protection for purely functional elements of buildings. Yet despite this general rule against protection of functional subject matter, the U.S. Congress chose copyright as the primary mode of protection for software. This choice has since led to enormous difficulties in applying copyright protection to software, since the primary value of software arises from its functionality.

For the past 25 years, courts throughout the U.S. have have struggled with the paradox of applying intellectual property protection that explicitly does not extend to functional items to an item that is primarily functional. The courts have attempted to accommodate software within copyright by excluding from consideration its functional aspects, applying copyright protection to only its expressive portions. But as one commentator has observed, any court honestly applying this test will find that nothing remains for its consideration after subtracting out the functional portions; everything in software is essentially functional.[2]

> JUST AS COPYRIGHT SEEMS TO HAVE EXPANDED TO ENCOMPASS FUNCTIONAL ITEMS, **PATENT LAW NOW SEEMS TO HAVE EXPANDED TO ENCOMPASS EXPRESSIVE SUBJECT MATTER.**

Nonetheless, copyright protection for software is sometimes justified by the argument that copyright also covers other representations of functional operations, such as choreographic notation, cookbooks, and how-to books. Each comprises an algorithm of some sort, such as the steps in executing a dance, steps in food preparation, and steps in repairing a toaster. Copyright also extends to blueprints and architectural drawings representing functional artifacts or buildings. Since the copyright statute defines software as "a set of instructions to a machine," the argument goes, software fits perfectly well alongside other instructional texts, such as choreographic notation, dictionaries, and blueprints or similar items.

Unfortunately, this argument demonstrates confusion of two very different definitions of "instruction"; instructions to a human are not the same as instructions to a machine. The instructions in a cookbook may say to add one teaspoon of baking soda to a recipe, but the human reading the instructions has the option of not adding the baking soda,

[1] *Baker v. Selden*, 101 U.S. 99 (1879).

[2] Karjala, D. A coherent theory for the copyright protection of computer software and recent judicial interpretations. *U. Cin. L. Rev.* 66 (1997), 53.

adding some different amount, or substituting another ingredient, such as baking powder. A machine executing instructions has no such latitude, because the software instructions literally become part of the machine performing the operations they embody. Choreography, dictionaries, and blueprints do not configure humans in the manner that software configures hardware; blueprints may tell humans how to build a machine, but software *is* the machine. No one would mistake choreographic notation for the dance or the blueprint for the building. Instructions to a human may be useful, but they are not functional in the same sense as software.

Following this distinction, some might suggest that source code, like a blueprint, represents a machine or building, while object code is analogous to the machine or building itself. According to this argument, human-readable source code would perhaps be the proper object of copyright protection, whereas machine-readable object code is not. But U.S. courts early in the development of copyright protection for computer software rejected this distinction. As a technical matter, the distinction is blurred and difficult to apply for interpreted languages, such as Basic and Java, and for hybrid languages, such as Perl. As a legal matter, if a programmer in fact fixes copyrightable expression, it makes no difference whether the expression is fixed as source code or as object code, just as it would make no legal difference whether copyrightable expression in a sculpture were fixed in steel or marble. As a purely practical matter, it would make little sense to protect the "expressive" source code version of a program without protecting the "functional" object code version, since mass-marketed programs are generally distributed in the latter form; outside the "open source" movement, a program's source code is typically held as a closely guarded secret, and its object code is most likely to be pirated.

This point—that there is no practical difference between source and object code for these purposes—becomes even clearer when we consider the fundamental interchangeability of software and hardware. For reasons of cost and efficiency, society has tended to deploy universal machines that can be configured by software to perform a variety of tasks. But we could also hard-wire machines to perform the same tasks, substituting hardware for software. Society has also chosen to place software within the subject matter of copyright, though no one would concede that the equivalent hardware falls within the purview of copyright. On the contrary, if two computer scientists were to present, respectively, for registration to the U.S. Copyright Office the software code for a particular application and a machine hard-wired to perform the equivalent function, the Copyright Office would readily accept the deposit of the code but reject the hard-wired machine. The hardware version would likely be turned away with the advice, much like that in *Baker v. Selden*, that hardware and similar functional items are the provenance of patent law, not copyright.

Software and Patent

Because patents cover utilitarian articles, it seemed natural to many observers that patent would be the form of intellectual property best suited to cover software. Patentable subject matter includes machines, processes, compositions of matter, and articles of manufacture that are novel, useful, and nonobvious. Unlike copyright, which arises spontaneously when a work is fixed in a tangible medium, a patent is obtained by submitting an application to the Patent Office. The application must describe how to make and use the claimed invention and contain one or more claims delineating the invention covered by the patent. Once the patent application is approved, the inventor may, for a period of 20 years, exclude others from making, using, selling, offering for sale, or importing the claimed invention.

The protection of software under copyright, rather than solely under patent law, is something of a historical accident. During the 1970s, the U.S. Supreme Court considered the patentability of software, initially declaring it unpatentable under a rule that prevents the patenting of abstract ideas or formulae.[3] In the view of the Court, algorithms seemed to constitute such abstract ideas or methods, placing software comprised of such algorithms outside patentable subject matter. The Court revisited the issue in 1981, amending its position to hold that software by itself was unpatentable but, if tied to some physical component or substrate, could be patentable.[4] This ruling led to elaborate judicial tests to determine the substantiality, or embodiment, of computer programs, as well as to the widespread practice by patent attorneys of claiming software in terms of the state of the machine configured.

Throughout the 1980s and 1990s, as applications for software patents became more common

[3] *Gottshalk v. Benson*, 409 U.S. 175 (1972).
[4] *Diamond v. Diehr*, 450 U.S. 175 (1981).

and the importance of the technology increased, lower courts incrementally stretched the Supreme Court's standard to cover more and more types of software. These courts had little difficulty in at least nominally tying software to a physical substrate, as the Supreme Court had required. To constitute patentable subject matter, software needed simply to produce some physical change in a machine—something a program unquestionably does; the execution of each step in an algorithm places the hardware in a different electrical or magnetic state. Thus, in one case, the stored data in a standard form of computer memory was held to be patentable, since the storage of the data placed the machine in a different state from the one it would otherwise have been.[5] Similarly, storing data or software code on a magnetic disk has been recognized as producing a novel and patentable article of manufacture, because the disk with the stored data differs from the disk without it. Under this approach, software might be claimed as either a "machine" or as a "process," because the algorithm produces a sequential series of different machines.

In the process stretching patent law to accommodate software, the courts went to some lengths to alter or discard certain rules of patent law that would tend to exclude software from being patented. For example, the courts have long held that mere arrangements of lines or symbols would not constitute patentable subject matter. Such "printed matter" was not considered to constitute patentable machines, manufactures, or compositions of matter. Novelty in substance, language, or meaning of printed indicia was similarly considered unpatentable. This is not to say that an invention would be unpatentable simply because it was printed on paper or some other substrate. Rather, to meet the criteria for patentability, the claims must define new features of physical structure or new relations of printed matter to structure. So, for example, some methods of fraud prevention involving detachable menu or railway tickets were held patentable, because they were tied to a physical cardboard ticket structure involved in the claimed process.

This rule tended to reinforce the dividing line between the functional and the aesthetic by removing literary or artistic works from the realm of patents; a poem or painting might be novel and even nonobvious but was considered to be the proper subject of copyright, rather than of patent protection. Forms and labels that had as their sole point of novelty printed markings or indicia were held unpatentable by U.S. courts. So too, accounting or indexing methods involving novel arrangements of symbols on known substrates, such as paper, were unpatentable, as were methods of arranging directory names by phonetic groups when the novelty lay in the arrangements of the names.

JUST AS A WORK NEED NOT NECESSARILY COMMUNICATE WITH A HUMAN TO QUALIFY FOR COPYRIGHT, **A WORK DOES NOT NECESSARILY QUALIFY AS PROTECTED SPEECH EVEN IF IT COMMUNICATES A MESSAGE TO A HUMAN.**

Ironically, despite the dictum of the Supreme Court in *Baker v. Selden* that Selden should have sought a patent for his accounting method, the printed-matter doctrine would likely have denied the uncopyrightable accounting forms of *Baker v. Selden* patent protection as being unpatentable "printed matter" involving only an arrangement of marks and not operating on a physical substrate.

The requirement of a physical substrate for printed matter evolved into the Supreme Court's holding that software must be tied to a tangible embodiment to qualify as patentable subject matter. But the printed-matter doctrine potentially posed a severe impediment to the patentability of software, which at some level resolves to indicia or symbols written on a physical substrate, such as paper and magnetic media. The courts have now eliminated this impediment by requiring only a novel arrangement of indicia or structure in the substrate. The difficulty with this approach is that data and software are essentially indistinguishable; as one judge has observed, magnetic media or a compact disc containing music files are novel arrangements of indicia in a physical substrate.[6] Under current U.S. law, Selden's method of using accounting forms would likely be patentable subject matter, so long as it produced "a useful result," but so too would many

[5] *In re Lowry*, 32 F.3d 1579 (Fed. Cir., 1994).

[6] *In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994) (en banc) (Archer, dissenting).

other arrangements of symbols, including, apparently, word processing files and music CDs. Thus, just as copyright seems to have expanded to encompass functional items, patent law now seems to have expanded to encompass expressive subject matter.

Software As Speech

The hybrid nature of software has surfaced in an additional area of the law with important repercussions for the convergence of patent and copyright. In a series of recent cases, the courts have grappled with the issue of whether or not software comes under the protection of the First Amendment, that is, whether software constitutes protected speech. Several such cases have involved constitutional challenges to federal restrictions on the export of cryptographic software.[7, 8] More recently, the issue of First Amendment protection has been raised in a copyright case involving a program capable of circumventing the encryption controls on DVD-format movies; defendants in the suit argued that the program code, which was outlawed under an anti-circumvention statute passed in 1998 by Congress, is protected speech and the statute an unconstitutional prior restraint on such speech.[9]

In each of these cases, the fundamental question for the courts was whether software is primarily functional or expressive, that is, whether software is "speech." The question of what constitutes speech is not entirely new to First Amendment jurisprudence. The Supreme Court has previously considered whether activities as diverse as nude dancing, flag burning, even parade marching qualify as speech under the U.S. Constitution.[9] The Court has at times based its definition of speech on whether the activity is communicative, that is, whether it conveys a message to an audience. Yet conveying a message cannot by itself be the touchstone of First Amendment protection; the majority of people cannot perceive the message in many types of expression, as in, for example, modern art and atonal music.

The Court has indicated that such expressive activity is protected, even if understood by few if any recipients. Thus, the Court has at times tempered its communication requirement with the proviso that speech must convey a message to a particularized audience or entail the potential to convey a message to those who might acquire the knowledge to understand the message.[10]

To those familiar with programming, the status of software under such a test may seem obvious, at least for source code. Source code is certainly comprehensible to the audience of computer programmers, conveying ideas to other programmers. This argument for code as speech certainly carries with it some superficial appeal. Programmers are undoubtedly expressing something when they compose the code that comprises a program. They think carefully about what they are composing. That careful thought, some of which may involve very innovative ideas, is transposed into the notation of a computer language other programmers can read and decipher to extract the logic that went into its composition.

But as we have seen in the case of copyright, such attempts to map expressive paradigms onto what is primarily a functional item have been highly problematic. The fact that an engineer "reading" program code appears to be reading textual instructions, rather than tracing logic circuits, is an artifact of the medium from which the program is built; the engineer "reading" the program code is extracting design information from a functional machine that happens to be composed of text.

The same characteristics are shared to a greater or lesser extent by other functional items. My running shoes, automobile, table cutlery, and essentially every other object around me in an industrialized society is the embodiment of some artisan's or engineer's design. Thus, the final product of such industrial design choices, functional as they may be, in a sense "communicates" the ideas of its originating artisan or engineer and so could be said to constitute a sort of "speech." As the Supreme Court has noted in other contexts, it is possible to find some kernel of expression in almost any activity, including, for example, walking down the street or meeting one's friends at the shopping mall, though such a kernel is not sufficient to bring the activity within the protection of the First Amendment. Similarly, every human artifact contains some kernel of "expression," but we do not protect them all.

This First Amendment problem is in some sense the inverse of the problem encountered in copyright law; just as a work need not necessarily communicate with a human to qualify for copyright, a work does not necessarily qualify as protected speech even if it communicates a message to a human. Litmus paper conveys a message to a human, but that message is unlikely to qualify as protected expression under either the First Amendment or the Copyright Act. However, the courts have accepted that computer operating systems, which do not convey a

[7] *Bernstein v. U.S. Dept. of Justice*, 176 F.3d 1132 (9th Cir. 1999).
[8] *Junger v. Daley*, 209 F.3d 481 (6th Cir., 2000).
[9] *Universal City Studios, Inc., v. Reimerdes*, 82 F.Supp.2d 211 (S.D.N.Y. 2000).
[10] *Hurley v. Irish-Am. Gay, Lesbian, and Bisexual Group of Boston, Inc.*, 515 U.S. 557 (1995).

message to a human, may qualify as protected expression under either the First Amendment or the Copyright Act. Simultaneously, if either the litmus paper or the operating system produce a useful result, the paper or the system is now the proper subject matter of patent. This convergence of expressive and functional subject matter has brought us to the point that patent law now covers expression, as patent law increasingly extends to software-related patents, including systems of writing and for voice command recognition, not to mention magnetic or structural elements comprising expressive works.

Accommodating Patentable Expression

The peculiar nature of software now demands an accommodation between the law of patents and the law of free speech. But it seems likely that the law of patents is not prepared for this juxtaposition with the First Amendment and may need considerable adjustment after the fashion of copyright. Copyright may have provided a poor guide for accommodating software within the law of the First Amendment but may provide a better guide for accommodating the First Amendment within patent law. Unlike patent law, copyright law has long been required to accommodate free speech issues through, for example, the doctrine of "fair use."

COPYRIGHT MAY HAVE PROVIDED A POOR GUIDE FOR ACCOMMODATING SOFTWARE WITHIN THE FIRST AMENDMENT BUT MAY PROVIDE A BETTER GUIDE FOR ACCOMMODATING THE FIRST AMENDMENT WITHIN PATENT LAW.

In copyright, fair use serves a variety of functions. First, it is widely held to facilitate worthwhile uses of copyrighted works where the value of the use is exceeded by the transaction costs of negotiating a license. Under such conditions, an unfettered "right to exclude" might deter such valuable uses; the potential users of the work are unlikely to expend more time and money to locate the owner and negotiate a license than they can recover from the licensed use. The fair use doctrine allows the potential user to take the needed portion of the work and make use of it without seeking a license, bypassing the need for deterrent high-cost authorization.

A second, related purpose of fair use is to facilitate socially valuable uses of copyrighted works for which the value is not fully internalized. Commentary, criticism, parody, and other unauthorized uses of intellectual property may encourage public debate and help foster an informed populace, but this value is diffuse and accrues to recipients other than the user of the copyrighted work. In the case in which such positive externalities are present, social welfare would be increased by the use of the work, but potential users may be deterred from doing so because they will not assess the use by its full value. Only a portion of the value of the new work will accrue to the potential user, and transaction costs in excess of that portion will produce the kind of market failure described earlier. In order to encourage creation of the work, fair use may again serve to bypass licensing that appears excessively costly from the perspective of the potential user.

Because copyright has traditionally encompassed expressive subject matter, fair use also functions as a sort of safety valve between the purposes of copyright and the demands of the First Amendment. Copyright is a type of restraint on speech, that is, the property right in the expression restrains others in their use of that expression. The First Amendment typically prohibits such governmental "prior restraints," but in the case of copyright, governmental interference is constitutionally authorized. Fair use mediates between these apparently contradictory constitutional provisions, especially in the instances outlined earlier in which parody and criticism foster an aware and educated populace better able to participate in the exchange.

As copyright has increasingly been forced to deal with functional artifacts within its ambit, fair use has also become an important way to prevent copyright holders from dominating new markets or from impeding development of new products. For example, fair use has been employed to provide the necessary flexibility in copyright law to allow reverse engineering of copyrighted software. The creation of software compatible with a given operating system or application program may require examination of the program's structure in order to design an interoperable product. The utilitarian functions of computer programs lie in the public domain and may be freely copied unless patented, as outlined earlier. However, companies developing competing or complementary products necessarily

create a copy of the program being studied in the course of decompiling it to examine it. This copying during reverse engineering might be considered an infringement, but the courts have consistently held that making intermediate or temporary copies in order to study a program and extract its public-domain information is fair use.[11]

Although fair use has proved critically important for all these roles vis-à-vis copyright, no such doctrine has emerged to fulfill these roles in patent law. One would think that in the case of functional technology, no less than the case of nonfunctional expressive works, instances might arise in which market failure is present. The cost of locating a patent owner and negotiating a patent license might well deter a potential user from engaging in valuable social use of the claimed invention. In many cases, access to patented technology may also involve positive externalities, in which the social value of certain uses of patented technology may be too diffuse to prompt a potential user to seek a license. The conventional wisdom has long been that patent owners must be free to exercise a right to exclude potential users in precisely the manner that was not permitted to copyright holders. However, such conventional wisdom may have to change in the face of patents now including works that are either overtly expressive or that lie on the uncertain border between function and expression.

Conclusion

Software does not fit comfortably into the traditional legal categories for functional works or expressive works. The law of copyright, then of patent, and now of the First Amendment have been strained past recognition in order to accommodate this technology. Perhaps the most sensible resolution to this difficulty would be to place software into its own unique category—not of patent, copyright, or even protected speech—but one specially designed to fit the characteristics of this unusual legal hybrid. Unfortunately, it is likely too late to turn back the clock and take such a sensible step; so we may expect that legal institutions will continue to classify as either "functional" or "expressive" a technology that may be neither or both. C

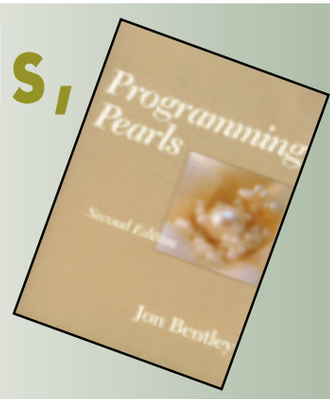
Dan L. Burk (burkx006@tc.umn.edu) is a professor of law at the University of Minnesota Law School in Minneapolis.

[11] *Sega Eters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

© 2001 ACM 0002-0782/01/0200 $5.00

Programming Pearls, Second Edition

by: Jon L. Bentley



Order #: 702003 Paperback 2000 256 pp.
ISBN: 0-201-65788-0
Members: $22.45 Non Members: $ 24.95
To order online: http://www.acm.org/catalog/

Call Toll Free:
1.800.342.6626 (USA & Canada)
1.212.626.0500 (outside US)
Fax: 1.212.944.1318

Association for Computing Machinery
The First Society in Computing

Randall Davis

THE DIGITAL DILEMMA

How intellectual property laws might embrace the apparently paradoxical goals of motivating individual creation and preserving the ultimate benefits of that creation for the common good.

The combination of technologies making up the information infrastructure—information in digital form, computer networks, and the Web—is accompanied by contradictory powers and promises. For intellectual property in particular, it promises more—quantity, quality, access, and markets—while simultaneously imperiling the rewards of those who create and publish it. It is at once a remarkably powerful medium for publishing and distributing information and the world's largest reproduction facility, running unchecked in practice, if not in statute. It is a set of technologies that can improve access to information enormously, yet can inhibit access in ways never before practical.

This set of technologies has arrived in a world in which our existing laws, policies, and practices governing intellectual property depend on subtle, surprisingly complex, and at times conflicting elements of law, public policy, economics, and technology. These elements are in relative balance today but may well be thrown out of balance by the transformations resulting from the information infrastructure.

One core of the problem is illustrated simply. A printed book can be read by one or perhaps two people at once, as long as they're located in the same place as the book. But make the same text available in electronic form, and there is almost no technological limit to the number of people who can access it simultaneously from almost anywhere on earth. At first glance, this is wonderful news for the information consumer and for society; the electronic holdings of libraries (and friends) around the world can be available 24 hours a day, year-round, and would never be checked out. These same advances in technology create new opportunities and new markets for publishers.

There is also a more troublesome side. Publishers and authors wonder how many copies of the work will be sold (or licensed) if networks make possible planetwide access? Their nightmare is that the number is one. How many books (or movies, photographs, or musical pieces) will be created and published online if the entire market might be extinguished by the sale of the first electronic copy?

The consumer nightmare, on the other hand, is that the authors' and publishers' attempt to preserve the traditional marketplace leads to technical and legal protections that sharply reduce access to our common intellectual and cultural heritage—resources long viewed as crucial to democracy and to science.

The information infrastructure thus has the potential to demolish the careful balancing of public good and private interest that has emerged from the evolution of U.S. intellectual property law over the past 200 years. The public good is the betterment of society resulting from the constitutional mandate to promote the "progress of science and the useful arts"; the private interest is served by the time-limited monopoly (a copyright or patent) given to one who has made

ROBERT NEUBECKER

a contribution to that progress. The challenge is in striking and maintaining the balance, thus offering enough control to motivate authors, inventors, and publishers, but not so much control as to threaten important public policy goals, such as preserving the nation's cultural heritage, providing broad access to information, and promoting education, science, and scholarship. As usual, the devil is in the details, and the past 200 years of intellectual property history have seen a largely successful, albeit evolving, balancing of these details. The evolving information infrastructure presents a leap in technology that upsets the current balance, forcing us to rethink many of our fundamental premises and practices.

The stakes are high, both economically and in social terms. Decisions we make today will determine who benefits from the technology and who has access to what information and on what terms—foundational elements of our future society.

It was in this context that in 1997 the U.S. National Science Foundation, prompted by a recommendation by the Federal Networking Council Advisory Committee, commissioned a study of the issues by the Computer Science and Telecommunications Board of the National Academies. The report, called *The Digital Dilemma: Intellectual Property in the Information Age*, published by the National Academy Press in February 2000, is the focus of this article.

WITH COMPUTERS NOW IN HUNDREDS OF MILLIONS OF HOMES WORLDWIDE, **INDIVIDUALS CAN DO IN PRIVATE WHAT NOT LONG AGO WOULD HAVE REQUIRED SUBSTANTIAL INVESTMENT AND PERHAPS CRIMINAL INTENT.**

Origins of the Problem

The difficulties we all face today arise primarily from two sources. One is a trio of technological advances that helped produce the infrastructure: the increasing use of digital information; the widespread reach of computer networks; and the creation of the Web. The second is the emergence of computers as a routine part of everyday life. These two developments have fundamentally altered the landscape, and their consequences present significant challenges.

Information in digital form. Information in digital form is orders-of-magnitude easier, faster, and cheaper to reproduce than is information in analog form (for example, hard copy). Digital copies are also perfect, so each one in turn can be the seed for additional perfect copies, quite unlike the situation with traditional media like photocopies.

These properties of digital information are for the most part widely appreciated by those familiar with computers. Somewhat less appreciated is the fact that accessing digital information inevitably means making a copy, even if only an ephemeral one. Such copying is deeply rooted in the way computers work. For example, when you view a Web page, several copies are made automatically, one so the document can be sent from the remote computer to your computer, a second when the document is loaded into memory, and yet another when it is displayed on the screen.

Such copying occurs with all digital information. Use a computer to read a book, look at a picture, watch a movie, or listen to a song, and you inevitably make one or more copies. Contrast this process with the use of traditional media; reading a book does not involve making a copy nor does watching a movie or listening to a song.

This intimate connection between access and copying is significant for intellectual property protection. One essential element of copyright—the right to control reproduction—works as expected in the world of traditional media, where there is an obvious distinction between access and reproduction and where the copyright owner's control of reproduction provides just that—control of reproduction. But in the digital world, where no access is possible except through copying, complete control of copying means control of access as well, a consequence of considerable importance to all stakeholders.

Networks and the Web. Computer networks have radically changed the economics and logistics of information distribution, enabling information to be sent worldwide almost for free and (for items of reasonable size) almost instantaneously. The Web in turn has radically altered the economics and logistics of publication, allowing everyone to be a publisher with worldwide reach. Where reproduction and distribution put information in the hands of those who know they want it, publication makes people aware of the information that is available, a function the Web performs well. The astonishing variety of documents, opinions, articles, and works of all sorts on the Web demonstrates that millions of people worldwide are making use of this capability.

This trio of technological developments—digital information, computer networks, and the Web—are together the source of profound changes in society. Digital information radically changes the economics and character of reproduction; computer networks radically change the economics and character of distribution; and the Web radically changes the economics and character of publication.

For publishers, these developments have opened up new markets and new product opportunities, including online music and books. But the same developments offer advantages to individuals and pirates making and distributing unauthorized copies; the process is orders of magnitude faster, easier, and less expensive than ever before. The important result is that the natural barriers to infringement have eroded significantly. Where unauthorized reproduction and distribution of hardcopy works is limited in part by the difficulty, expense, and loss of quality inherent in the process, with digital information, perfect copies can be made and distributed almost for free. Stakeholders on all sides of the issue wonder whether something can be put in place to restore the balance of forces or whether the world has changed fundamentally and permanently.

Commonplace technology. The second major source of difficulties in the digital dilemma is the routine presence of computers and the Web in work settings, and increasingly in households as well. Technology found only in research laboratories not long ago is now a widely available consumer product. One consequence is that individuals routinely have the means and opportunity to access and copy vast amounts of digital information, including software, text, and audio and video files, but lack a clear picture of what is legal or ethically acceptable. As a result, they are unprepared to deal with the associated intellectual property issues. Corporations dealing with these issues turn to their legal staffs, but individuals are bewildered, if indeed they are aware of the law at all.

A second consequence of the diffusion of the technology into everyday life is that intellectual property law and its enforcement are increasingly concerned with private behavior. Copyright has traditionally been concerned with public actions and their public consequences, such as public performance, public display, and distribution of copies. It has also focused on the behaviors of organizations and individuals whose actions have large-scale public consequences. But with computers now in hundreds of millions of homes worldwide, individuals can do in private what not long ago would have required substantial investment and perhaps criminal intent. As the potential impact of private behavior has grown, so correspondingly has interest in regulating such behavior. This shift in the focus of intellectual property law represents an important consequence of information technology's emergence into everyday life, thus presenting another social and policy challenge in managing the intellectual property balance.

Consequences of Licensing

One of the many problematic issues raised by the digital dilemma is the increasing use of licensing, rather than sale, as the primary mechanism for distributing information. Licensing is in some respects familiar; mass-market software has long been distributed via a (shrink-wrap) license, giving the purchaser a right to use the software but providing no ownership in it. More recently, a variety of digital information has been licensed, including documents, databases, and images.

There are significant differences between selling a work and licensing it. The sale of a physical copy of a work has been the dominant model for transferring intellectual property to the consumer for more than 200 years and involves the complete transfer of ownership rights in a particular copy of the work. Copyright law explicitly anticipates the sale of intellectual property products and, by its "first-sale" rule, gives the purchaser a significant body of rights with the purchased copy.[1] The purchaser is, for example, free to lend, rent, or resell the purchased copy. In that sense, copyright law follows intellectual property products into the marketplace and promotes the continued dissemination of information.

Licenses, by contrast, are contracts, that is, private agreements providing for limited transfer of rights to use an item. They can involve a range of terms and conditions but, unlike copyright law, need not incorporate any public policy considerations beyond some basic limits on what constitutes an enforceable contract. To the extent that digital information is distributed by license, there is no statute, history, or tradition of incorporating such public policy considerations as "fair use."[2]

Licensing can have advantages for all parties; it can provide clarity on terms and conditions of access, as well as increased rights for the institution beyond those provided under copyright, including the ability

[1]The first sale rule is contained in Section 109 of the Copyright Act, saying, in part: " ... the owner of a particular copy [of a copyrighted work] ... is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy..." It's called the first-sale rule, because the rights of the copyright owner over a particular copy of the work are extinguished by the first sale of that copy.
[2]Fair use is a legal principle enabling certain uses of copyrighted material, even in the absence of permission. Among the most familiar examples are the short quotes used by one writer when commenting on the work of another, as in, say, book reviews, position papers, and satires.

to make unlimited copies for local use. Licensing may also increase the options for making information available. For example, a license may grant time-limited access to some part of a book or report, perhaps for far less than the purchase price for the entire work.

But there are also concerns about the effect licensing may have on public access. Consider libraries as the archetypal example. In the print world, a library's failure to renew a subscription or buy an updated version of a book has no effect on the availability to patrons of earlier volumes or editions. In the world of licensed information, however, ending a subscription to an electronic publication may mean the end of access to earlier volumes or editions as well. While some libraries and publishers have worked to negotiate licenses that preserve fair use and other public-access features, concerns remain about the use of a mechanism lacking any of the built-in protections for public access embodied in copyright law.

> WHEN ACCESS REQUIRES REPRODUCTION, **THE RIGHT TO CONTROL REPRODUCTION IS THE RIGHT TO CONTROL ACCESS,** EVEN TO AN INDIVIDUAL COPY ALREADY DISTRIBUTED.

Questions also arise about the interaction of licenses and copyright. For example, copyright law today gives owners of copies of computer software the privilege to make backup copies. Can this privilege be taken away by a shrink-wrap license? Can a license term prohibit disclosing flaws to other potential users? These and related questions are far from being resolved.

If licensing becomes the dominant means of distributing information in mass markets, additional concerns arise for works considered part of our common intellectual and social heritage. One could imagine a world in which novels, poems, and paintings are available only (or mostly) by license rather than sale. The consequences for public access of such a world are far from clear.

Finally, the trend toward licensing means that increasing amounts of information are delivered as *experiences*, rather than as artifacts. This is not entirely unfamiliar; where books are information artifacts, first-run movies are information experiences. We have lived with both for some time, but the difference matters. Buy a book and you own it forever; pay for access to a digital book and when the period of service is over you often retain nothing.

Responses to the Dilemma

There are a variety of actions that can be taken in response to the challenges posed by this dilemma. I focus here on four: technological protection mechanisms, innovative business models, taking a broader perspective on the problem, and rethinking the nature of copyright.

Technological solutions. The key technical problem in large-scale management of digital information is determining how to provide access without giving up all control. A variety of clever schemes have been proposed, many relying on a combination of encryption and rights-management software. Encryption encodes information so it can be accessed only with the appropriate key; rights-management software enables fine-grain control of access, specifying such things as the number of accesses permitted and whether the material may be printed.

A common scenario for using encryption involves making it both machine-specific and persistent. Encryption can be made machine-specific by incorporating into the encryption process some reliable property of the decryption/playback device. For a computer, for example, the serial number of the hard drive or CPU might be used. Then, even if both the file and encryption key are passed on to others, the information remains inaccessible because it cannot be decrypted on machines with different identifiers.

But what if the original purchaser decrypts the information and passes it on to others? Persistent encryption tries to prevent this from happening by narrowing as much as possible the window of opportunity during which the decrypted information is available, even to an authorized user. In this approach, information is decrypted just in time, that is, just before it is used, making it available only as briefly as possible, and then only in small chunks at once. It is never stored, even temporarily.

Rights management involves providing some indication of the rights the consumer has purchased; this information is either encrypted along with the content itself or possibly maintained on a separate "rights server" accessed over the Web. Software on the user's machine then controls access to the information, consulting the rights listing to determine whether a

requested action is permitted.

Technological solutions can be useful but are limited in a number of important ways. One constraint arises from the need for consumer devices to be simple and fast. In some cases, this fundamental need precludes the use of industrial-strength encryption, which, though nearly impossible to crack, may be too slow for some consumer uses. However, the less-powerful encryption systems used in commercial products (such as the content-scrambling system used to encrypt DVDs) have been cracked.

Second, anchoring content to a specific machine raises an interesting problem for consumers: What happens when you upgrade your computer (or other playback device)? Must you repurchase everything you bought previously?

Finally, there is substantial difficulty in attempting to provide end-to-end protection within a general-purpose computer. PCs have been successful to a significant degree because they have open architectures; that is, components of the machine (such as the hard drive and the video card) are accessible to the consumer. As long as the machine is designed this way, decrypted information can be intercepted and captured as it passes from one place to another inside the machine. Hardware and software designers could make such steps progressively more difficult, but the effort they would have to expend, and the consequential costs for all involved, would be substantial.

Business models. In general, although technology can play a useful role as a deterrent to unauthorized copying, it is far from a panacea. Consider, then, a second possibility: the use of innovative business models. By selecting an appropriate business model, a rights holder can at times significantly influence the pressure for and degree of illegal commercial copying and unauthorized reproduction.

Several general principles offer insight into the sorts of business models that can help. One principle suggests making the product cheaper and easier to buy than to steal. The point is to reduce the motivation to deal with unauthorized sources from the outset. Music provides an example; single tracks can be bought online for 99 cents. But why pay even a dollar for something you might be able to get for free? Because, even with peer-to-peer programs (like Napster and Gnutella), the music isn't really free; there's an investment of time and effort in finding and downloading it. With the informal, all-volunteer effort at the heart of all the file-sharing schemes, the difficulty of finding what you want may be substantial, and the time required to download (from an overloaded personal computer in a dorm room somewhere) may be significant.[3] Would you pay a dollar to avoid the hassle? Quite likely. Hence, even beyond the obvious issues of ethics and legality, the answer to "Why pay?" is: for service, reliability, and speed.

A second general principle suggests reconceptualizing the basic product. As noted, the digital music business may be primarily a service business, rather than a product business. As the value in the digitized music itself becomes increasingly difficult to protect (all digital information is difficult to protect without losing control of it), the value may reside in providing speed, reliability, and ease of access, rather than in artifacts like CDs or tapes.

A third principle is illustrated by writer Stephen King, whose publication *The Plant* appeared online in installments beginning mid-2000 with unrestricted downloading of the installments. King warned, however, that if too few people actually paid for their downloads, the installments would stop coming. This is intellectual property approached not as law, but as economics (pay or it dies) and as sociology ("no stealing from the blind newsboy," in King's elegant description).[4]

These general principles suggest that thinking about the digital information business in innovative ways leads to a number of nontraditional business models. Importantly, each of these models creates an environment in which there is significantly less need for intellectual property protection:

Give away the product; make money from an auxiliary service. The Linux operating system, for example, is given away, yet a number of companies are in the business of providing service, consulting, customization, and extensions to the organizations using it.

Give away the product; sell upgrades. Many antivirus vendors make available free, fully functional versions of the programs on their Web sites. They give them away in order to sell subscriptions to the regular updates they add to their antivirus databases.

Give away one piece that promotes another. Adobe gives away its Acrobat Reader software to popularize the Acrobat PDF format and to create a market for all its other programs that create PDF files.

Offer extreme customization. Custom CDs with a particular customer's selection of audio tracks are likely to be a less appealing target for reproduction.

---

[3]Looking for a song by Neil Young and can't find it? Try looking for "Niel Young" instead.

[4]At press time, the experiment had been suspended for a variety of interesting reasons; see Mr. King's explanation at www.stephenking.com/sk_120400_2.html.

Offer a mass-market product at a low price and high volume, along with frequent improvements. Many software products fit in this category. Keeping the price low reduces the pressure for piracy, while constant improvement means the damage from unauthorized reproduction is time-limited.

None of these models solves the problem completely, but each one can sharply reduce the need for intellectual property enforcement.

There is also a more general point here about the relative power of law and business models: Although legal prohibitions against copying are useful against large-scale pirates, they are unlikely to be nearly as effective against individual infringers, where detection and enforcement are problematic. Where such private behavior is concerned, business models may offer a far more effective means of dealing with intellectual property issues.

AS THE TURMOIL IN THE MUSIC, PUBLISHING, AND MOVIE INDUSTRIES SUGGESTS, THE UPHEAVAL CREATED BY NEW TECHNOLOGY MAY MEAN THAT ACCOMMODATION IS NOT ENOUGH.

Multiple perspectives. The problems arising from the interaction of intellectual property and the information infrastructure need to be considered in a context encompassing not only law, technology, and markets, but economics more generally, as well as psychology and public policy.

This multiplicity of views is important in three ways. First, each of them brings a fundamentally different approach and mindset to the problem. As all of them are relevant, there is power in considering each different conception of the problem. Second, some disagreements arise because the positions are grounded in different perspectives (such as law, rather than economics) and are thus, in effect, asking (and answering) different questions. Finally, being aware of the multiplicity of perspectives may open additional routes for dealing with the issues; not every problem needs to be legislated into submission.

Is copy still the right concept? One final response to the digital dilemma asks this fundamental question about intellectual property. All of the preceding discussion accepts a fundamental perspective underlying copyright, namely, copying as a foundational legal and conceptual notion. As the very name of the law indicates, the right to control reproduction is central to copyright. Deciding whether a work has been copied has, as a result, been a fundamental issue underlying much of copyright history and analysis.

But is the notion of copy still an appropriate conceptual framework in the age of digital information? Two reasons suggest it might not be. One, as discussed earlier, is that legitimate use of a digital work *requires* making a copy. Hence, noting that a copy has been made tells far less about the legitimacy of the behavior than it does in the hardcopy world, where there are few legitimate rationales for copying an entire work.

A second is that, because copying is so bound up with the way computers work, controlling the act of copying, in the view of some legal scholars, provides unexpectedly broad powers, considerably beyond those intended by the copyright law. In the world of physical works, once a work is published, the rights holder cannot in any pragmatic sense control access to the copies distributed. Social institutions (such as bookstores and libraries) and individuals with copies enable any motivated reader to gain access to the information in the work.

But when access requires reproduction, the right to control reproduction is the right to control access, even to an individual copy already distributed. Authors would not, of course, routinely deny access to their published digital works. But because access requires reproduction, control of reproduction provides control of access to individual published copies, a right not conceived of as part of copyright, and hence not to be embraced lightly, whether or not it's routinely exercised.

Considering that control of reproduction is a means, not the goal, can we find some other mechanism more tightly connected to the goal of motivating individual contributions to progress in science and the arts, whether in the digital or analog world. Finding such a mechanism is not easy, but one suggestion may help promote serious consideration of the issue.

It may be useful to start not by asking whether a copy has been made, but by considering what the law is attempting to achieve—ensuring progress in the arts and sciences. We should therefore ask instead whether a use being made of a work is substantially destructive of a common means of achieving that goal, namely, providing incentive to authors. This approach is similar in overall spirit to the concept of fair use, which requires consideration of the effect on

the market for the work or on the value of the work. But it is somewhat broader in scope, as incentive arises for authors in more than the marketplace alone, coming as well, for example, from the ability to control the time, place, and manner of publication.

This view would not conflict with all of the other traditional exclusive rights in copyright. Creation of derivative works, distribution, public performance, and display of the work can all be conceived of and protected on grounds independent of whether a copy is made. They also affect incentive, whether through economic effects in the marketplace or through other factors, and hence would be consistent with an incentive-based analysis.

Any such substantial change in the legal framework would also, of course, bring problems. Therefore, there would have to be a substantial period of familiarization, as well as a means of dealing with the tension between trying to make such a law easier to follow (by drawing a sharp line defining what constitutes incentive-destroying use) and keeping the criteria more general (as is the case for fair use), allowing the law to address unanticipated situations in the future. Nevertheless, the discussion and examination of what constitutes a well-grounded model of intellectual property protection in the digital world may be well worth the effort.

Looking Ahead

The development and deployment of the information infrastructure presents a variety of challenges, ranging from the pragmatics of enforcing laws that can be casually broken by individuals (in private, inexpensively, and almost undetectably), to the possibility and perhaps the need to rethink some of the foundational concepts underlying these laws. Yet, from its origins in the patent laws of Venice in the 1400s through to modern times, intellectual property law has evolved and changed in response to such challenges. What is likely to happen this time? Several things.

To some degree, society will simply adjust to the new reality and carry on in familiar ways. Recall how software vendors gave up on the awkward technical mechanisms used in the 1980s to defeat piracy (such as distributing their products on disks that could not be copied in the ordinary way) and continued to do business and prosper in a world where there is nontrivial piracy. So it is likely to be with the distribution of digital content. Customers will grow increasingly used to subscriptions to online information, and authors and publishers will continue to do their work in the presence of some unauthorized reproduction.

But as the turmoil in the music, publishing, and movie industries suggests, the upheaval created by new technology may mean that accommodation is not enough. New business models will need to be explored and tested. New approaches to intellectual property issues will need to be founded on more than law and technology, embracing as well an understanding of the economics of information, sociology, and psychology. Intellectual property itself may need to be reconceptualized to some degree, in recognition of the changes we now face.

The issues are difficult but inescapable. We are all unavoidably engaged in an experiment that tests our ingenuity and resourcefulness in finding ways to accomplish the apparently paradoxical goals of motivating individual creation while still reserving the ultimate benefits of that creation for the common good. And we need to do so in a world where replication, distribution, and publication are astonishingly easier and less expensive than they have ever been. These issues are as important as they are difficult; the decisions we make today will shape foundational elements of our future society. C

RANDALL DAVIS (davis@ai.mit.edu) is a professor in the computer science department at MIT in Cambridge, MA.

© 2001 ACM 0002-0782/01/0200 $5.00

Rocky Mountain College
Dept of Computer Science

Computer Science: Rocky Mountain College, Billings, Montana, a small liberal arts college with approximately 800 students and an average class size of fifteen, is seeking an Assistant Professor Computer Science. This is a tenure-track position starting in August 2001. Responsibilities include teaching undergraduate ACM curriculum courses, advising, serving on committees, and curriculum development. Preferred candidates will teach database management, software engineering and algorithms, as well as lower level intro courses. Distance education experience is desirable. Master's degree required, Ph.D. preferred. Submit letter of interest, vita, teaching evaluations (if available) and a list of three references to:

Bob Robertson, Director of Personnel
Rocky Mountain College
1511 Poly Drive
Billings, MT 59102.

E-mail queries to: wierb@rocky.edu. Position will be open until filled. AA/EOE

THE BATTLE OVER THE INSTITUTIONAL ECOSYSTEM IN THE DIGITAL ENVIRONMENT

How U.S. law, by adding exclusive private rights to information, favors traditional industrial production of information products and discourages the emerging culture of Net-based peer production.

The 1990s saw a series of technological shocks to the economic and technological ecosystem within which information is produced. These shocks—declining communication costs, increasing efficacy and availability of processing power, and manipulability of digitized information—challenged the dominance of the large-scale industrial information producers that flourished in the 20th century—Hollywood, the recording industry, and various publishing giants. They also brought about a Cambrian explosion of new types of information producers and new models of information production that now challenge the dominance of the incumbents. Volunteers of all types began to fill the Internet with information, knowledge, and cultural exchanges. From amateur weather observation posts to Viking heritage societies, from academic courses to online political discussion forums, small-scale, widely distributed information production and dissemination have taken root and now represent a serious alternative to the more tightly controlled, better-ordered information environment of only 10 or 20 years ago.

The centerpiece of the emerging species of information production is free software and its apolitical offspring: open source development. On top of volunteerism and "peer production"—by peer users who organize by communicating with each other, rather than through market mechanisms or managerial hierarchy—free software has provided "organization" in the sense of the common pursuit of purpose and measurable efficacy. Organization and efficacy, in turn, suggest the possibility of economic sustainability and, more dramatically, the potential superiority of the new model of information production over the old. If Apache, GNU/Linux, Perl, and Sendmail are better than their proprietary competitors, then the mode of information produc-

tion they represent deeply challenges our assumptions about the social value of the industrial information producers of the 20th century.

Institutional Parameters

Since the mid-1990s, we have seen an intensifying battle over the institutional parameters of the ecosystem within which these modes of information production compete. Most important, the effort to define the new parameters has meant a struggle over intellectual property rights. In the U.S., we have seen a vast expansion of rights in multiple dimensions. The term of copyright was lengthened. Patent rights were extended to cover business methods. Trademarks were extended by the Federal Anti-Dilution Act of 1995 to cover entirely new values, becoming the basis for liability in the early domain-name trademark disputes.

The most extreme reshaping of the legal landscape has involved the introduction of new legal tools with which information vendors can now hermetically seal access to their materials to an extent never before possible. The Digital Millennium Copyright Act of 1998 (DMCA) prohibited decryption of the encryption preventing access to digitized materials. The Uniform Computer Information Transactions Act (UCITA), which has so far been passed in two states and is being considered by others, validated clickwrap licenses. Together, these laws permit vendors of information products to control access to their products free of the inconvenient balances that U.S. copyright law has always included, such as "fair use," which gives users rights to use copyrighted materials without permission in a variety of circumstances.

For example, the fair-use doctrine under traditional copyright law permits a critic to quote a 30-second clip from a videotape in order to criticize it. If the video is delivered in encrypted digital format (as are DVDs), however, under the DMCA, it becomes illegal for the critic to quote the 30-second clip. The reason is that, in order to quote, the critic must decrypt the copy-protection code. In the recent DVD case *Universal City Studios v. Reimerdes*, a federal district court in New York held that the DMCA does not include a fair-use defense for decryption. The DMCA prohibits decryption of copyright-protection measures, except for a narrow set of exceptions, and absolutely prohibits creation or distribution of utilities for this type of decryption, apparently without exception. The court held that the U.S. Congress purposefully sacrificed the privileges of users, primarily those relying on utilities created by others, to secure the rights of the copyright owners. The upshot of the case is that by encrypting their digitized information products, vendors can exempt those products from the user privileges—like fair use—that U.S. copyright law has always secured.

Similarly, if a clickwrap license prohibits reverse engineering of the software it covers, the UCITA and several recent court cases would enforce that contractual provision. By doing so, the owner could deny to other developers the privilege to reverse engineer where it is considered a fair use under traditional copyright law and even where it is expressly permitted by the DMCA. That enforcing such licenses vitiates the balance struck by copyright law has left many legislators and judges unconcerned.

Contraction of the Public Domain

On another front, a debate is raging over legal protection for compiled data involving contraction of the public domain. Contraction does not follow, as with the DMCA and UCITA, from letting owners determine their own access rules, but by formally making private that which previously was in the public domain. Since the U.S. Supreme Court's 1991 decision in *Feist Publications, Inc. v. Rural Telephone Services Co., Inc.* it has been understood that raw data is in the public domain and cannot be protected by copyright. Both the Copyright Act of 1976 and the Constitution left the unoriginal aspects of a database, that is, the raw data, free for use in the public domain. Copying data from an existing compilation was therefore not "piracy." It was not unfair or unjust but purposefully privileged in order to advance the goals of intellectual property—the advancement of progress and creative use of the data.

Since *Feist*, the larger players in the database

publishing industry have pushed Congress to pass a law that would, as a practical matter, overturn *Feist* and create a property right in compiled raw data. Because *Feist* was a constitutional decision, these efforts are disguised as creating not an intellectual property right in unoriginal data but as an "unfair competition" law. However, the law that has been introduced repeatedly walks, talks, and looks like a property right.

Most important, the proposed law applies to value-adding users, not solely to free-riding competitors, as an unfair-competition law would. The congressional committee that supported the bill stated, for example, that a person compiling a database of public-domain photographs of famous people in Massachusetts would have a claim against another person combining parts of the same database with similar databases from other states to create a national portrait gallery. This kind of trade-off between past information producers and future information producers is at the heart of intellectual property but has little to do with unfair competition.

ONLY COMPANIES WHOSE BUSINESS MODELS DEPEND ON LICENSING RIGHTS **REAP THE BENEFITS OF STRONG RIGHTS.** EVERYONE ELSE SIMPLY HAS TO PAY HIGHER PRICES FOR INPUT.

Moreover, the proposed new exclusive rights in data extends to repeated access for the purposes of gleaning one or two facts at a time. Information production that relies on automated search programs to collect information from existing sites will likely run afoul of the proposed database protection law. They will continue to exist, if at all, at the sufferance of the sites being searched in this manner.

It is precisely the right to prevent this type of information collection that eBay, not waiting for Congress to move on database protection, succeeded recently in persuading a federal district court in California to invent for it out of common law whole cloth. In *eBay v. Bidder's Edge*, the court found that by crawling eBay's site in search of information about what is up for auction there, Bidder's Edge—an aggregator of data on what is available for auction on various sites—perpetrated a form of trespass. This holding (or a federal database law expanding its effect nationally) would threaten to make illegal many such automated information-collection techniques.

Tilted in Favor of Industrial Production

To understand how the expansion of exclusive private rights in information tilts the institutional ecosystem within which information is produced against peer production and in favor of industrial production, consider the following examples, one real-world, one hypothetical.

The real example is the *Los Angeles Times v. Free Republic* case. In 1999, the *Washington Post* and the *Los Angeles Times* persuaded a federal district court in California that individual users should not be permitted to cut and paste stories from their online editions onto a political discussion forum in which they participated. The Free Republic Web site is a gathering place for conservatives; one service it offered was a forum in which users would post newspaper stories with comment, and others would continue to comment on the piece. The Free Republic forum presents an alternate information universe; its end points are peer users, rather than consumers of finished packaged goods. "Quality" in this world is created not by "professionalism" but by shared values, by knowing one's interlocutors and conversing with them, and by the sheer number of users scouring the world, looking for things on which to comment.

The court found that by enabling users to share stories they found at the New Republic site had violated the newspapers' rights and prohibited them from sharing the stories as part of their political discourse. To reach this conclusion, the court assumed that public discourse is best served by increasing incentives to professional, commercial producers relying on copyright to sell their products, even at the expense of individual users thereby prevented from engaging in public discourse.

The result of interpreting law to serve the commercial/professional producer was to burden access for the peer producers of news and commentary—the forum participants—to the raw materials needed for their common enterprise. The decision is a quintessential instance of a self-fulfilling perception of the world. It began with an assumption that there are active commercial producers and passive consumers, and that consumers are better off when producers have strong incentives to produce. It then shaped law to make the production and dissemination of news and comment more lucrative for commercial producers and more hostile and

costly for amateur or volunteer producers.

To understand the effect in more detail, consider the following hypothetical example of the implications of the proposed database-protection law. Imagine that a company invests in collecting genealogical information intending to bundle it in a family-software pack for distribution with home computers. Under present law, if an enthusiastic fourth-grade teacher decides to take the information in the database and write a program to allow his or her students to create personalized family trees with photos they bring from home, the teacher is perfectly privileged to do so. Copyright law leaves the raw genealogical information in the public domain precisely in order to allow and encourage such creative reutilization. The new database law would, however, require the teacher to get permission from, and pay, the original compiler of the genealogical data.

It is important to understand that this law would cause producers like the teacher to avoid engaging in creative efforts *inefficiently*. When the teacher is deciding whether to write code to customize the database for the students, the genealogical information has already been collected; no new resources need be expended to allow the teacher to use it. The social cost of the teacher using that information is therefore zero. This is what economists mean when they say that information is a public good.

The only real social cost of the teacher's developing the utility for making a personalized photo-integrated family tree is his or her own time and effort. Under present law, the teacher can decide to invest this effort out of dedication to his or her work, for the joy of creativity, or, if he or she is more calculating, for the positive effects on his or her personal reputation. With the new law, the teacher would also have to factor-in the price of using the data—a cost that from a purely economic perspective is inefficient for the teacher to take into consideration. If he or she decides that spending the time and effort (the actual social cost of development) is worth it but cannot pay for the data, because, for example, neither the teacher nor his or her school has the budget to buy it, the teacher would not write the additional code. Given that the teacher is willing to invest the time and effort, the decision not to develop the program because of the cost of using the data is inefficient.

The problem is not specific to databases. It applies more generally to exclusive private rights in information. As information or cultural products—with the same public-goods economic characteristics as raw data—become more completely enclosed by intellectual property rights, the public-domain contracts. Small-scale or noncommercial producers deciding whether to produce some information or cultural element face the same difficulty as the teacher in the example. Only companies whose business models depend on licensing rights reap the benefits of strong rights. Everyone else simply has to pay higher prices for input.

Moreover, when intellectual property rights are extensive, owning a large inventory gives owners relatively cheaper access to raw materials than is available to producers who do not own large inventories; they can reuse their own materials, as well as those available to all from the public domain. This means that commercial organizations that integrate new information production with ownership of large inventories of existing information do better in an environment with very strong property rights than either noncommercial organizations or other commercial organizations that do not own large inventories. Industrial information producers (such as the major movie studios) are the greatest beneficiaries of stronger property rights because of the way they organize their productive enterprises. Their gain comes at the expense of other modes of production, most extensively at the expense of peer production.

Potential for Profound Social Transformation

The emergence of free software-like productive enterprises and nonprofit production of culture, knowledge, and information (both professional and amateur) presents the potential for a profound social transformation. The 19th and 20th centuries were dominated largely by one major social-political problem—figuring out how freedom, productivity, and justice could be attained in a material world. Contemporary Western capitalism eventually triumphed over all its alternatives—anarchism, communism, fascism, as well as 19th-century laissez-faire capitalism—by adhering to a particular conception of freedom that political philosophers call "negative liberty," separating questions of productivity from questions of freedom and putting productivity ahead of justice. The success of our current social and economic system has been so overwhelming that we increasingly view it as the best of all possible worlds.

However, the combination of economic evolution toward an economy focused on information production and exchange and our technological shift toward digitally networked communication

changes the fundamental parameters around which the settlement of contemporary Western capitalism has congealed. The economics of information production and exchange are fundamentally different from the economics of physical goods. This is not a millenarian statement or utopian vision; it simply states the basic economic understanding that information is fundamentally different from physical stuff as an object of economic activity.

What has failed to materialize in our public discourse is a debate over how this change in a central part of our productive activity challenges our social-political settlement. Liberal democracies developed their prevailing answers to the question of how shall individuals be free, productive, and live in a just society when the core resources and outputs in their economies (such as coal, ore, and grains) were scarce traditional economic goods, costly to produce and distribute. They found that organizing production under these conditions requires boxing freedom into the categories of "public-political" and "private-personal," keeping both to a great extent out of the productive realm. We discovered that too much focus on equality could lead to a serious decline in productivity, to the serious compromise of freedom, or both. But these answers no longer have the same purchase when the most valuable inputs and outputs of our society—information, knowledge, culture, and human creativity—are either public goods in the strict economic sense or uniquely personal to creative, nonfungible individuals.

PROPERTY IS A HINDRANCE, NOT AN AID, WHEN PEER PRODUCTION OF A PUBLIC GOOD LIKE INFORMATION IS POSSIBLE.

The point is that simply copying the settlement from the economy of stuff to the economy of information is unnecessary. In that portion of our lives increasingly occupied by information, we can be free in a richer sense and more egalitarian in the distribution of wealth while maintaining or increasing productivity.

At the root of the economic—and ultimately social—transformation is a change in the menu of options for being effective and productive in the information economy. In the atoms economy, we settled more or less on two modes of making production decisions. The first was the market; the second was corporate hierarchy. Some economic activities were best coordinated by markets; others were better organized by managers. The result was that most individuals lived their productive lives as part of corporate organizations, with relatively limited control over how, what, or when they produced; these organizations, in turn, interacted with one another through a combination of markets and hierarchy. Consumption was strictly separated from production for most people and largely devoted to receipt of finished goods, not to creative utilization of materials to shape one's own environment.

Sustainable Peer Production

Emerging now in the information economy is a model of peer production. Individuals communicate with one another about which projects are worth pursuing and who might want to take them up; they share their products in an economy of gifts, reputation, and relationally based rewards. Consumption and production are integrated, not separated, so each individual is a "user," rather than either purely a "producer" or "consumer."

The possibility of sustainable peer production is not mushy wishful thinking. That much, at least, is demonstrated by Apache, GNU/Linux, Perl, Sendmail, and other free software programs.

In peer production, low-cost continuous information exchange replaces price signals and hierarchical commands as the primary mechanism of cooperation and coordination. Low-cost communication, enabling thousands of individuals to collaborate on complex projects, is therefore a necessary precondition to the emergence of peer production as a third mode of organizing production, distinct from either markets or hierarchies.

The other necessary precondition is low-cost access to the universe of existing information that is the raw material from which new information goods are made. The capacity of thousands to scour a rich universe of existing information resources allows them to identify productive opportunities and the creative individuals who can best use these resources. That capacity is the primary source of productivity gains that peer production offers our economy. It is here, too, that the ecological competition between the industrial, large-scale producers of yore and the peer producers of today kicks in. If large-scale commercial producers (relying on some mix of market and

hierarchy to coordinate production and appropriate the benefits of their enterprises) can enclose much of the universe of useful information inputs with newfangled property rights, contracts, or encryption, then they can seriously limit the viability of peer production as a widespread, sustainable alternative mode of production. The squelching of peer production is at the heart of today's legal battles over intellectual property.

Political Economy in Systematic Imbalance

These battles suffer from a systematic imbalance. The incumbents gain and internalize all the benefits from new rights. Their gains are concentrated, and they view them as private gains unto themselves. The costs to peer users—in terms of increased cost of access to information inputs—are diffuse and to be incurred largely in the future. Those who are destined to pay them after a new right is created are dispersed, many not seeing themselves at the time of legislation as implicated by the law. Just as the fourth-grade teacher in the earlier hypothetical example about databases would be unlikely to participate in the database-protection legislative process. This systematic imbalance leads to a process of legislation that steadily increases the scope and extent of exclusive private rights in information, with occasional carve-outs for specific constituencies that happen to be well organized and recognize at the time of legislation that they will be adversely affected by the law.

The consequences of the legislative imbalance could be devastating to peer production, the emerging species of information production. While peer producers may be equally or even better able to set the technological parameters of the environment in which they compete with the large incumbents, setting the technical parameters alone will likely be insufficient. A Linux DVD player depends on legally permissible access to DVD encryption. It is not enough that the encryption can be cracked. For Linux DVD players to become widespread, *legal* access is necessary. As long as the large-scale industrial information producers can persuade legislators and judges that their existence depends on hermetically sealing all access to all information materials, as they did in the DMCA and in the *Universal City Studios* DVD case, legal access to the raw materials necessary for peer production will be denied.

What peer production needs to flourish is a space free of the laws developed to support market- and hierarchy-based information production. In the late 18th and early 19th centuries, market-based production was replacing artisan and guild-based production, and the common law developed the framework—modern property and contract law—that transition needed. The guild masters resisted, but law changed. In the late 19th and early 20th centuries, larger-scale production in corporate hierarchies was necessary to coordinate the complex production decisions that technology had made possible. Law developed to accommodate these properties by developing corporate law, antitrust law, labor law, and securities law. Some of these newer laws conflicted with and displaced contract and property law, as in the power corporate law gives managers to make decisions independent of the wishes of "the owners" of the corporation (its shareholders) and as labor law displaces traditional contract law.

Entering the 21st century, our law must again develop to accommodate another newly emerging mode of production, this time peer production. Here, the primary need is to develop the legal framework for sharing and exchanging information among peers whose interaction is not based on exclusion requiring property rights. Property is a hindrance, not an aid, when peer production of a public good like information is possible. Law must instead adapt to develop a series of sustainable commons in the information environment.

Whether law shall permit peer production to emerge has social importance well beyond the importance of any single use. Such use could be a particular program or even free software as a phenomenon peculiar to software production, as opposed to as a template for peer production of information more generally. A peer-produced environment both requires and enables a legal framework that increases the diversity of information available to people in society and decreases opportunities to control political processes and individuals' personal choices. A robust public commons in which all can speak to all and collaborate with all in sharing perspectives on how the world is and how it could be enhances our political self-governance as well as our individual self-governance, that is, our autonomy.

Can Freedom Resolve into Anarchy?

Risks, too, are associated with this freedom. Traditionally, we have relied on various points of control, including corporate boards, community ethics, and law, to ensure that freedom does not turn to anarchy and that diversity of voices does not turn to cacophony. Where shall community and order come from in the new, free environment? Some of

the established peer-production systems, including university research, and the newly emerging peer-production systems (such as free software) suggest that freedom does not resolve into anarchy in the absence of trenchant organizational control of the corporate or state-based varieties.

People develop community standards and mutual reliance and monitoring that rely on the media in which they communicate to one another, doing so as part of the peer-production processes. Common efforts that lack mechanisms for self-ordering fail as productive enterprises and as structures for organizing social life. We should therefore focus our legal design interventions to facilitate self-ordering of distributed peer-production communities.

The transformation will therefore not be to a world in which no one is responsible to anyone else, and no standards apply to one's behavior other than one's own. There will be neither a libertarian nor an anarchist utopia. But there could be incremental and significant improvement in autonomy and self-selection in each of our social relations, and more authentic social organization.

Conclusion

We are in the midst of a pitched battle over the spoils of the transformation to a digitally networked environment and the information economy. Stakeholders from the older economy are using legislation, judicial opinions, and international treaties to retain the old structure of organizing production so they continue to control the empires they've built or inherited. Copyright law and other intellectual property, broadcast law, spectrum-management policy, and e-commerce law are all being warped to fit the size of the hierarchical organizations of yesteryear. In the process, they are stifling the evolution of the distributed, peer-based models of information production and exchange.

As economic policy, letting yesterday's winners dictate the terms of tomorrow's economic competition is disastrous. As social policy, missing an opportunity to enrich our freedom and enhance our justice while maintaining or even enhancing our productivity is unforgivable. C

Yochai Benkler (yochai.benkler@nyu.edu) is a professor and director of the Information Law Institute at New York University School of Law.

© 2001 ACM 0002-0782/01/0200 $5.00

ACM Fellows

(continued from page 76)

Nomination information organized by a principal nominator includes:

1. Excerpts from the candidate's current curriculum vitae, listing selected publications, patents, technical achievements, honors, and other awards.
2. A description of the work of the nominee, drawing attention to the contributions which merit designation as Fellow.
3. Supporting endorsements from five ACM professional members.

ACM Fellows nomination forms and endorsement forms may be obtained from ACM by writing to:

ACM Fellows Nomination Committee
ACM
1515 Broadway, New York, New York 10036-5701, USA
nominate-fellows@acm.org

The forms can also be accessed from: www.acm.org/awards/nomination_packet/
Completed forms should be sent by August 31, 2001 to *one* of the following:

ACM Fellows Committee
ACM
1515 Broadway, New York, New York 10036-5701, USA
or
nominate-fellows@acm.org
or
+1-212-869-0824 - fax

A. Michael Froomkin

THE COLLISION OF TRADEMARKS, DOMAIN NAMES, AND DUE PROCESS IN CYBERSPACE

The increasingly uneasy coexistence between the Internet's domain-name system and established trademark law raises questions about whether the Internet's regulations are technically expert or democratic and fair.



The domain-name system (DNS), which plays a key role in routing the large majority of Internet traffic, was designed at a time when there were few hosts and the pre-Internet network was limited mostly to academic users, researchers, and non-commercial traffic. The idea of giving internetworked computers easily remembered names dates back at least to 1971 when Peggy Karp, an early author and editor of the network engineers' Requests For Comments, prepared the first hosts.txt file, the predecessor of the modern "root" file. Each version of the DNS since then has sought to provide routing efficiency, ease of use, and the ability to scale, although it's unlikely many of the founders foresaw quite how much it would need to scale. Today, with a substantial part of the name-resolution infrastructure still provided on a volunteer basis (and the name assignment function increasingly regulated and commercialized), the DNS continues to meet its objectives of providing mnemonic-to-IP mappings while preventing name collisions on the Internet. It thus undergirds part of the network's fundamental technical stability.

Technical success, however, has bred social issues. In the mid-1990s, the DNS and the people admin-

ROBERT NEUBECKER

istering it were blindsided when copyright and trademark holders decided the DNS collided with naming systems in "meatspace," or the part of life that is not cyberspace, especially with trademark law. The manifold consequences of this perceived collision have already included U.S. legislation, strange doings by various international bodies, the creation of the Internet Corporation for Assigned Names and Numbers (ICANN), plus the invention of a unique and idiosyncratic arbitration system with troubling due-process problems. It is no exaggeration to say that this crash of two collision-avoidance systems has shaped—perhaps one could say misdirected or even warped—the governance of the Internet.

Trademark law is organized around a set of objectives and assumptions that map incredibly badly onto the Internet, and even worse onto an Internet that uses the current DNS. Trademarks (and service marks) are intended to be a user-friendly shorthand for an expected level of product attributes, such as quality. Trademark law seeks to protect consumers from fraud, counterfeiting, and confusion, as well as the goodwill businesses build up in their trademarks. If someone passes off inferior goods by affixing a competitor's trademark or something that looks confusingly similar to it, both consumer expectations and supplier goodwill suffer.

Throughout most of the world, trademarks are acquired solely through registration with the appropriate government department. In some countries, however, notably the U.S., "common-law trademark" rights can also be acquired through use, without the formality of registration. Like domain-name registrations, trademark reservations have a first-come-first-served aspect to them, though the similarity is limited.

Traditionally, trademark law is organized predominantly on sectoral, geographic, and national principles. The exception is a small class of "famous" names (such as Coca-Cola) where the assumption is that consumers in the region in which the mark is famous would reasonably associate the name with any type of goods on which it might appear. Otherwise, the guiding principle behind a great deal of trademark law is that it achieves its purposes best by limiting the reservation of rights in a name (or symbol or other identifier) to the type of goods and location where these goods are sold. Thus, "Joe's Pizza" can get a trademark in the town where it sells pizza, not for the whole state or the whole country; different Joe's Pizzas can dot the landscape as long as they do not serve overlapping territories. If one Joe's Pizza becomes a national business, it cannot undermine the preexisting rights of the Joe's Pizzas already extant, but it can more or less prevent them from expanding their markets. Similarly, Apple Computer coexists internationally with Apple Records because these businesses offer different classes of goods and services.

In short, trademark law is designed to allow multiple, concurrent use of the same name by different people in the same business in different places or by substantially different businesses in the same place. Trademark law is national law geared to local and regional conditions, supported by a set of international treaties in which most nations agree to allow foreigners to acquire domestic trademarks and give these marks equal treatment with other domestic marks.

THE MODERN DOMAIN-NAME CRISIS REALLY BEGAN WHEN **A SMALL BAND OF SPECULATORS DISCOVERED THEY COULD REGISTER NAMES CORRESPONDING TO TRADEMARKS,** THEN TRY TO RESELL THEM TO TRADEMARK HOLDERS FOR LARGE PROFITS.

In contrast, the organizing ideas of the Internet are worldwide nondiscriminatory access and layered protocols to enable provision of seamless service to the user and flexibility to the developer. The DNS is organized around two complementary hierarchies, one to register names and ensure their uniqueness, the other to resolve names to the dotted-quad IP numbers actually used to route Internet traffic. The DNS used by most Internet users requires that only one person have a single second-level domain (SLD) in each top-level domain (TLD) and that all TLDs be unique. (There are "alternate roots," or different data hierarchies for resolving mnemonics to IP numbers, though only a small fraction of Internet users avail themselves of them.)

Until recently, legal issues relating to the DNS were barely on the technologists' radar, and the primary objective in the few early RFCs that even addressed intersections between the DNS and the legal system was to find an external rule administered by someone else that could be included by reference as a sort of social function call. As a practical matter,

Internet pioneer Jon Postel fixed the list of TLDs in 1984 [10]; it has hardly changed since then, other than the addition of a few new country codes. (ICANN plans a rollout of seven new, somewhat limited, TLDs in 2001.)

Postel delegated authority to register names in TLDs on a more or less first-come-first-served basis. In .com (and soon after in .org and .net), second-level domain names went to whoever asked for them first. Other TLDs imposed more restrictive criteria, but most also allocated second- or sometimes third-level names to the first qualifying applicant. As late as 1994, when the DNS design had already substantially evolved into the form it has today, RFC 1591 said little on the now-vexed question of domain names and trademarks. Similarly, on the equally explosive question of the creation of two-letter country code TLDs (ccTLDs), such as .us, .tv, and .tm, RFC 1591 said: "The IANA [Internet Assigned Numbers Authority] is not in the business of deciding what is and what is not a country" [9].

Soon after RFC 1591 was published in 1994, businesses started rushing to establish their presence on the Internet, prompting a rapid increase in commercial and near-commercial uses, including corporate PR. In this new environment, a system optimized for its technical virtues and easy mnemonics crashed into trademark law. The pressure on the DNS grew rapidly because businesses decided that .com was the best TLD; moreover, they came to believe that for practical purposes, only one person or firm could have "its" name on the Net. And, whether or not .com was the only TLD that mattered to business, the number of gTLDs and ccTLDs open to anyone with the money was certainly far smaller then the number of Joe's Pizzas or persons or firms named McDonalds.

Strangely, most of the defining domain-name conflicts have not been between competing trademark holders with the same name in different trademark classes nor between firms with the same name in similar trades located in different places. The modern domain-name crisis really began when a small band of speculators—quickly dubbed "cybersquatters"—discovered they could register names corresponding to trademarks, then try to resell them to trademark holders for large profits. As attractive domain names in .com began to be scarce, more and more speculators began to register names. Until July 1999 when .com names could be registered with no money down and 30 days or more to pay, domain-name speculation seemed a low-risk, potentially high-reward business. (Indeed, it is believed that in January 2000, the Bank of America bought "Loans.com" for $3 million; see www.canoe.ca/TechNews0002/09_loans.html.) As the speculators moved from generic names to names that equaled, resembled, or contained trademarked words belonging to large and small corporations alike, disputes over domain names became increasingly common, spilling over into the court system. For example, courts in both the U.S. [7] and England [2] held that such registrations of trademarked words, for the purpose of resale to a trademark holder, constituted actionable trademark infringement. At least in the U.S., the correctness of this result was debatable, since both the Lanham Act and the Federal Anti-Dilution Act require "commercial use" of a term before it becomes actionable; perhaps seeking to do rough justice, courts found commercial use in the attempt to sell the names.

Even with the law on their side, trademark holders were increasingly worried and unhappy for three reasons. First, trademark law imposes a substantial burden of monitoring on the holder of a mark. Failure to contest adverse use can result in the loss of all or part of one's trademark rights; this need to police trademark rights makes intellectual property lawyers err on the side of aggressiveness. Second, even a successful federal court case is expensive in money and management time; domain-name speculators understood this, and the gap between a $100-or-so registration fee and the several-thousand-dollar cost of prosecuting even an uncomplicated case represented a substantial profit opportunity. And third, businesses slow to come to the Internet found the names they wanted were already registered to others; since these names worked everywhere, they necessarily worked in the locations where the business with the trademark was established, even if the domain-name registrant was in the same line of business far away.

The obvious technical solution to this problem was to create new TLDs so everyone could have the second-level domain names they wanted. But that only threatened to make the first two problems worse. Postel and others proposed creating several hundred new TLDs, but opposition from firms holding large numbers of valuable trademarks blocked the plan.

The conflict eventually got the attention of the White House and the U.S. Congress. In June 1998, the U.S. Department of Commerce issued a white paper *Management of Internet Names and Addresses* calling for the U.S. to hand off most of its operational control of the DNS to a private nonprofit company [11]. It also identified cybersquatting as a major problem in need of action by the new entity; in the interim, it also called for the U.N.'s World Intellectual Property Organization (WIPO) to pro-

vide the new body with advice on what it should do.

The U.N.'s WIPO duly convened an elaborate process and produced a lengthy report that, after proposing a maximalist trademark agenda in its initial draft, settled for requesting only most of the loaf [3, 12]. Notably, WIPO sought the authority to create a registry of famous names it would control. Only the holder of the famous trademarks would be allowed to have domain names corresponding to these names, even if other users (especially noncommercial ones) would have had a right to use the names offline, as was routinely the case.

Congress also got into the act, ultimately passing the Anticybersquatting Consumer Protection Act (ACPA) of 1999, which created new rights for trademark name holders against domain-name registrants [1]. It authorized courts to levy up to $100,000 in statutory damages against cybersquatters, regardless of the plaintiff's actual damages; in practice, the major result of this provision likely was to pressure registrants to surrender domain names, rather than risk the danger of such a large fine. ACPA also created a new "in rem" cause of action though which plaintiffs could ask a court to transfer a domain name (but no fines) even if they were unable to locate the registrants or if the registrant lived outside the jurisdiction of the U.S. courts. However, like other trademark law in the U.S., ACPA applied only to commercial users of a trademarked term; parody, criticism, and other traditionally protected uses remained protected [1].

Meanwhile, the Department of Commerce, which had become the lead government agency for DNS policy, decided it would prefer not to mediate between the dot-coms calling for new TLDs and the trademark holders arguing against them. Instead, it decided to "privatize" the DNS—coincidently removing itself from the line of fire—calling for the formation of a nonprofit corporation to take over the DNS. That call was quickly answered by the founders of ICANN. Although ICANN's makeup, its somewhat secretive origins, and various aspects of its bylaws all caused controversy, Commerce soon signed a number of contracts with ICANN, giving it day-to-day control over the DNS and effectively making it the regulator of registrars and registries in .com, .org, and .net [4].

Commerce charged ICANN with technical coordination of the DNS but also instructed it to do something about cybersquatting. In so doing, it ensured that despite a formal mandate limiting ICANN to technical coordination, ICANN would inevitably be in the more controversial business of Internet governance [4]. Although ICANN did not accept WIPO's suggestion regarding famous names, it did adopt in October 1999 a modified version of its plan for mandatory arbitration of domain-name disputes it called the Uniform Dispute Resolution Policy (UDRP) [6]. In the UDRP, ICANN imposed on all current and future registrants in .com, .org, and .net a requirement that they agree to a third-party beneficiary clause in favor of any person, anywhere, who believes a registrant's domain-name registration infringes the complainant's trademark right.

THE PROCEDURES USED BY THE UDRP SUFFER FROM SUBSTANTIAL DUE-PROCESS FLAWS—THAT WOULD HAVE MADE THE PROGRAM OBVIOUSLY ILLEGAL IF THE U.S. GOVERNMENT HAD ATTEMPTED TO IMPLEMENT IT DIRECTLY RATHER THAN HAVE IT DONE VIA ICANN OR SOME OTHER ARMS-LENGTH PRIVATE BODY.

This clause is not optional; ICANN's contracts with registrars requires them to include this clause in every registration contract they enter into and to modify existing contracts with their customers; registrars failing to do so would then find their registrations refused. Under the UDRP, a complainant with a trade or service mark has the burden of demonstrating three facts:

- That the domain name is identical or confusingly similar to the registrant's use of the domain name;
- That the registrant has no rights or legitimate interests in respect of the domain name; and
- That the domain name was registered and is being used in bad faith [6].

The UDRP provides a nonexhaustive list of factors constituting bad faith, including registering in order to sell it to the mark holder, and some defenses, including legitimate noncommercial use.

The UDRP offers much to trademark registrants seeking to claim domain names from registrants, as the proceeding can cost under $1,000 for a panelist, depending on the complainant's choice of dispute-resolution provider. The arbitration runs on a very fast track, with each side only allowed to offer one short pleading with exhibits attached. Save in the most exceptional case—which has yet to occur—there is neither a live hearing nor online argument. Proceedings normally take 45 days or less from complaint to conclusion. Respondents who lose have 10 more days to file a challenge in a competent court; otherwise, the domain name is transferred to the complainant [6]. It is no surprise then that almost 4,000 cases have been filed under the policy since it began in mid-1999; of those that have proceeded to a decision to date, more than 75% have been decided for the complainant [8].

The UDRP's advantages to complainants come at the cost of a substantial reduction in registrants' legal rights. First, rather than both sides having equal input into who decides the case, the complainants choose the arbitral tribunal from a list of approved providers maintained by ICANN. Respondents have no say in which provider will mange the case nor peremptory challenges to arbitrators they may fear are biased. Respondents can, however, pick one member of a three-person panel—at their own expense if the complainant opted for a single panelist and the respondent decided three are needed [5]. Overall, the system gives dispute-resolution providers an economic incentive to compete by being complainant-friendly [8].

The UDRP does not require actual notice to respondents, only attempted notice for a relatively short period of time [6]. The mere sending of the complaint to postal mail, fax, and email addresses found via whois (an Internet directory service based on domain-name registration records), and by email to postmaster@<*the contested domain name*>; any email address shown or email links on www.domain-name suffices to start the 20-day clock for the respondent's only chance to reply. The decision to forgo requiring actual notice in absolutely all cases is understandable, given the efforts the sleaziest registrants pursue to hide their contact details in shady registrations. The short deadlines, on the other hand, are completely unfair. Respondents who happen to take a three-week vacation without email can lose their chance to explain why they should keep their domain names without ever knowing it was endangered.

Most significant, the consequences of the arbitration discriminate against registrants. UDRP decisions are not "binding"; if the complainant loses, the arbitration does not preclude an attempt to bring the case in court [6]. "Nonbindingness" is a feature, not a bug; a summary procedure in which each side has only one submission and in which there is no testimony, cross-examination, briefing, or argument cannot by itself hope to make reliable determinations or sort out complex competing claims. If the system can, by design, resolve only uncomplicated cases of trademark infringement, it follows that complainants with more complex cases should lose but should still be entitled to their day in court—where sometimes they deserve to prevail.

The problem is that losing respondents are much worse off than losing complainants. Losing registrants have to sue to keep the name, taking on the burden of proof and possibly being subject to different courts, rules of procedure, language, and choice of law than if the complainant had been forced to litigate in the judicial district in which the registrant resides. Worse, under the UDRP, a losing respondent is given just 10 days to file an action in a court with jurisdiction over the complainant—or in the jurisdiction in which the registrar is located—to halt the transfer of the domain name [5]. No injunction is needed, as mere filing of an ordinary complaint suffices to stop the clock. But the requirement that the losing registrant file a complaint within 10 days still means that either the losing respondent must have hired and probably paid a lawyer in advance or the loser needs to find representation in a hurry.

This process contrasts very unfavorably with the choices facing a losing complainant, who has as much time to go to court as allowed by statutes of limitations or laches (an equitable principle barring delayed claims when the delay unduly harms the defendant), possibly months or even years. The rule has particularly harsh effects in such legal systems as the one in Mexico that restrict, or even prohibit, amendments to complaints once they are filed; the rule means the domain-name registrant who loses a UDRP arbitration has less than 10 days to find a lawyer and work out his theory and statement of the court case and no chance to correct errors or omissions caused by the rush.

These problems show that the procedures used by the UDRP suffer from substantial due-process flaws—that would have made the program obviously illegal if the U.S. government had attempted to implement it directly rather than have it done via ICANN or some other formally arms-length private body [4]. Worse, although the UDRP's basic substantive rules—representing the sort of compromise that leaves both sides unhappy—are probably fundamentally sound, what's written down has less

effect than one would expect.

The dirty secret of the UDRP is that a noticeable fraction of the arbitrators don't follow the rules as written. For example, as noted earlier, the UDRP states that complainants must have a trademark in order to bring a complaint, that the domain name must be identical or confusingly similar to the trademarked term, and the respondent must have no legitimate right to use the name. Each of these requirements has been ignored with sufficient frequency as to make the rapid and inexpensive UDRP seem an attractive gamble to some parties engaged in "reverse domain-name hijacking" seeking to obtain a domain name they would not be able to get in court.

On paper, U.S. federal trademark law after the most recent amendments is more favorable to trademark plaintiffs than the UDRP. Yet arbitrators under the UDRP have been willing to find names—like directlinesucks, dixonssucks, freeservesucks, guinness-beer-really-really-sucks, guinness-really-really-sucks.com, natwestsucks, standardcharteredsucks, and walmartcanadasucks—are "identical or confusingly similar" to a trademarked term without the "sucks." Under standard trademark principles, it is very unlikely that a court would find that a consumer would be likely to think these terms indicate sponsorship by the company being mocked.

> RESPONDENTS WHO HAPPEN TO TAKE A THREE-WEEK VACATION WITHOUT EMAIL **CAN LOSE THEIR CHANCE TO EXPLAIN WHY THEY SHOULD KEEP THEIR DOMAIN NAME** WITHOUT EVER KNOWING IT WAS ENDANGERED.

Yet the arbitrator in the walmartsucks.com case concluded it "is by no means necessarily" so that the name "would be recognized as an address plainly dissociated from" Wal-Mart. Although the arbitrator allowed that "Some will treat the additional 'sucks' as a pejorative exclamation and therefore dissociate it after all from the complainant," he seemed to think that some people were not clever enough to make this distinction and would be "confused." Courts usually have a more robust view of consumers' IQs.

Moreover, in the U.S., most of the "sucks" sites would be constitutionally protected speech, even if they were potentially confusing, as long as they were purely noncommercial.

The first year's experience with the UDRP has revealed flaws in need of urgent correction. However, the outlook for reform is somewhat cloudy, since ICANN has yet to announce how it will conduct its review, currently scheduled for some time in 2001. Meanwhile, WIPO is pressing ahead through a series of reports and meetings that may call for increasing the UDRP's current (relatively narrow) scope to cover a much wider variety of claims relating to domain names, including those based on place names and personal names.

Over the next 10 years, the domain-name problem may be self-limiting. There is no technical bar to the creation of thousands, even tens of thousands or more, of new TLDs. Domain names themselves may become less important, as search engines and other means of finding Internet hosts become smarter and more ubiquitous. As the Internet becomes more deeply woven into society, many of the current, transitory problems—predominantly caused by established businesses first discovering the Internet—will become rarer and less controversial.

The more serious problem, however, lies at a more fundamental level. The DNS wars put in question not only who should be in charge of resolving the very uneasy coexistence between trademark law and the DNS but also future collisions between Internet technology and the legal regimes that order the rest of our lives. One way to resolve these problems is to decide that the Internet is not unique, letting the courts and legislatures get on with their jobs. Indeed, in the U.S. and elsewhere, these institutions have begun to do so, albeit with mixed results. Worse, the solution is slow and sometimes expensive. Trademark owners are not one of the least powerful groups in our society, and they eloquently, and often persuasively, argue that they were being taken advantage of while the law evolved its solutions, including ACPA. The search for interim or generally more nimble relief has led some trademark interests to advocate new solutions based in quasi-governmental and semiformal processes, including WIPO's domain-name initiative and ICANN.

ICANN's UDRP is a rapid, lightweight, inexpensive process allowing victims of cybersquatting to vindicate their rights (in practice, more than their rights) far more cheaply and quickly than would be possible in most courts. However, ICANN is a private, nonprofit corporation purporting to be little

more than a standards body engaged in "technical coordination." Yet the UDRP is not in any ordinary sense "technical coordination" of the Internet. It embodies a policy choice to sacrifice the interests of (some) domain-name registrants in favor of (some) trademark registrants for the sake of a vision of the communal good.

While this policy choice is surely one a legislature could make, it is not at all evident that Congress or any other legislature in the world ever made it nor that U.S. law allows the Department of Commerce to outsource policymaking to private bodies like ICANN [4]. Similarly, overreliance on WIPO's advice raises concerns. While undoubtedly expert, WIPO is neither democratic nor nonpartisan, as it exists to further the protection of intellectual property. The procedures WIPO uses to produce its recommendations make it likely that its work product will state a consensus of intellectual property rights holders, rather than a broader view [3].

Therefore, there is substantial risk that the chief long-term fallout from the collision between domain names and trademarks will be to institutionalize decision-making processes that are neither expert technical processes applied to true standards matters nor particularly democratic or fair. C

References

1. Anticybersquatting Consumer Protection Act, Pub. L. No. 106-43 ß 3(a)(2), 5, 113 Stat. 218, 220 (1999).
2. *British Telecommunications plc and another v One In a Million Ltd and others* and other actions [1998] 4 All ER 476, [1999] 1 WLR 903, [1999] RPC 1; see www.bna.com/e-law/cases/ukspencer.html.
3. Froomkin, A. Semi-private international rulemaking: Lessons learned from the WIPO domain name process. In *Regulating the Global Information Society,* C. Marsden, Ed. Routledge, London and New York, 2000; see www.law.miami.edu/~froomkin/articles/tprc99.pdf.
4. Froomkin, A. Wrong turn in cyberspace: Using ICANN to route around the APA and the Constitution. *Duke Law J. 50,* 1 (2000), 17–186.
5. ICANN. *Uniform Domain-Name Dispute Resolution Policy*; see www.icann.org/udrp/ udrp-policy-24oct99.htm (Oct. 24, 1999)
6. ICANN. *Rules for Uniform Domain Name Dispute Resolution Policy*; see www.icann.org/udrp/udrp-rules-24oct99.htm (Oct. 24, 1999).
7. *Intermatic, Inc., v Toeppen,* 947 F. Supp. 1227, 1237-40 (N.D. Ill. 1996)
8. Mueller, M. Rough justice: An analysis of ICANN's uniform dispute resolution policy. *Info. Soc.* (2001); see dcc.syr.edu/roughjustice.htm
9. Postel, J. *RFC 1591, Domain Name System Structure and Delegation*, Internet Engineering Task Force; see www.ietf.org/rfc/rfc1591.txt (Mar. 1994).
10. Postel, J. and Reynolds, J. *RFC 920, Domain Requirements I*, Internet Engineering Task Force; see www.ietf.org/rfc/rfc0920.txt (Oct. 1984)
11. U.S. Dept. of Commerce. Management of Internet names and addresses. *Fed. Reg. 65* (June 10, 1998), 31,741–31,751; see www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm.
12. World Intellectual Property Association. *The Management of Internet Names and Addresses: Intellectual Property Issues, Final Report of the WIPO Internet Domain Name Process*, 1999; see wipo2.wipo.int/process1/report/finalreport.html.

A. Michael Froomkin (froomkin@law.tm) is a professor or law at the University of Miami School of Law.

© 2001 ACM 0002-0782/01/0200 $5.00

HARVARD UNIVERSITY
COMPUTER SCIENCE

Lecturer on Computer Science

Applications and nominations are invited for a Lectureship on Computer Science to work with faculty in teaching introductory courses in computer science. Candidates should be outstanding teachers of computer science with extensive experience in classroom instruction and a record of creativity and achievement in teaching and curriculum development.

Details of the position will be tailored according to the strengths of the successful candidate but would include activities such as curriculum development, lecturing, course administration, and supervision of section leaders. The Lecturer would be involved in introductory programming and theory courses each semester, working individually and with other members of the faculty.

The position will begin as early as the 2000-01 academic year and offers an opportunity to work with outstanding students in excellent teaching facilities housed in a recently completed new building. Lecturer positions are annual appointments, renewable for up to three years. Applicants must have a Ph.D. in Computer Science or a related discipline.

Information about Harvard's current faculty, research, and educational programs in the Division of Engineering and Applied Sciences, which includes the computer science program, is available at:

http://www.deas.harvard.edu/.

Candidates should send a curriculum vitae and a statement of teaching experience and interests, and should also arrange to have at least three letters of reference sent to:

CS Lectureship Search Committee
Division of Engineering and Applied Sciences
Harvard University
Maxwell Dworkin 247
33 Oxford Street
Cambridge, MA 02138

Applications will be reviewed as they are received.
Harvard is an Equal Opportunity/Affirmative Action employer and encourages applications from women and members of minority groups.

Early applications advised.

IS VIRTUAL TRESPASS AN APT ANALOGY?

Despite the appeal of equating virtual and real property rights, providing relatively open Web access is likely to yield a more vibrant Internet.

Legal doctrine often evolves both more slowly than the conduct and the technology it is intended to regulate and by analogy. When parties argue that previously unheard-of behavior should generate some legal response, the relevant institution (generally Congress, the courts, or administrative agencies, such as the U.S. Patent and Trademark Office) often seeks guidance from past experience. Earlier decisions addressing a specific factual context give some confidence that applying the legal rules from these prior situations to the new fact pattern will produce a sensible result.

But principles developed to deal with one set of facts can only imperfectly fit another. This imperfect fit often becomes more evident over time, sometimes raising the question of whether the initial analogy itself was valid. Legal doctrine may then evolve away from its first response to a new condition toward more specific rules reflecting an increased appreciation of the points at which the original analogy does not hold.

For example, the U.S. courts that first addressed claims of software copyright infringement in the 1970s and 1980s and Congress, when it decided to include computer programs within the category of "literary works" under the Copyright Act, analogized writing computer programs to writing novels. However, over time, the courts began to have difficulty using this analogy to apply rules developed with books and manuscripts in mind to software. In particular, long-established law held that a novel's plot, if sufficiently detailed, is protected by copyright. Courts found it difficult to translate this "old" law into the new context of computer programs in which the "plot" is much more difficult to see and understand. Additionally, market realities demand that other programs connect to the initial copyrighted one as, for example, Lotus 1-2-3 and Excel each run on top of Microsoft's Windows. Moreover, any PC operating system that hopes for any chance of marketplace success must run at least the set of applications run by Windows, the dominant system. Achieving compatibility may necessarily result in similarities between the "plots" of the original and the compatible programs. Should a court hold the author of the later-developed program an infringer?

Initially, the courts granted fairly broad protection to program structure.[1] Over time though, as they began to appreciate how computer programs differ from traditional literary works and to understand the economics of the software industry, they developed

[1] See, for example, *Whelan Assoc., Inc. v. Jaslow Dental Lab., Inc.*, 797 F.2d 1222, 1236 (3d Cir. 1986) (holding that the unprotected idea of a computer program is its overall purpose, and that all parts of the program's structure not necessary to the implementation of the idea are protected by copyright).

MAUREEN A. O'ROURKE

new rules specific to software to define the extent of copyright protection for a program's "plot."[2]

While software copyright cases continue to be difficult to adjudicate, the law has at least evolved to some measure of stability. The Internet is now the legal frontier on which the process of setting rules by analogy and adjustment is just beginning. Courts have begun to grapple with questions like who may access a Web site, in what manner, and for what purpose. Their resolution of these issues will greatly influence the structure of competition on the Internet for the foreseeable future.

They represent a difficult challenge, because the law has never before dealt with rights of access to a medium like the Internet or "property" like a Web site. But courts have historically addressed such questions as who may enter another person's land or use another's chattel (personal property that is tangible, but, unlike land, also portable) under trespass law. This time-tested legal doctrine, at least at first glance, seems to provide an apt analogy for adjudicating legal claims based on unauthorized access to and use of Web site data.

Closer analysis reveals, however, that an unthinking transplantation of tangible property law to the Internet is likely to create some undesirable results. This article explains why Web sites seek to limit access to and use of their information, why the principles of real and tangible personal property law present attractive analogies, and why use of these prior rules of decision is inappropriate without adjustment. It concludes by proposing some factors courts should consider in evaluating claims whose gravamen reduces to charges of unauthorized access to and use of Web site data.

Limiting Access to Web Sites

The notion of limiting access to Web sites may seem odd to those who recall the Internet as a research network where open access and the free exchange of scientific information was the norm. It was, however, inevitable, that as commercial firms began to turn to the Internet for revenue, they would begin to view their Web sites as valuable "real estate" to be protected against those who would use their existence or content to make money for themselves. Indeed, while the reasons a site owner may wish to limit access to its site are as numerous as Web sites themselves, a large percentage may be classified under the broad heading of preventing "free-riding" by others that threatens the visited site's revenue model in one way or another.

The most obvious example of a site that would literally have to limit access to continue in business is one that relies on subscription revenue for its existence. If nonsubscribers are legally permitted to circumvent the subscription and payment process, the site's primary revenue stream is dissipated. Similarly, some sites provide certain data for free but impose a charge for access to additional information. If visitors can avoid the fee and obtain the "restricted" information anyway, the site's revenue stream disappears.

Other, perhaps less obvious examples, exist. Regardless of their revenue model, some sites may limit access to certain of their parts to users who have met certain qualifications. For example, a porn site may limit access to interior pages to those providing some assurance that they are 18 years of age or older.

Many sites continue to generate at least part of their revenue from advertising, often charging others for the privilege of placing banner ads on their home pages. The advertising rates are usually set with reference in some way to the number of "hits," or visits to the home page.[3] If another site links directly to interior pages, the visited site may lose revenue, because no hits to the home page are recorded. Sites may be reluctant to take technological steps to block deep linking because the linker may circumvent the block. The linker's practical ability to overcome virtually any technological barrier may lead to a "technological arms race" in which the site continually builds higher fences only to have the linker knock them down. Indeed, the increasing number of lawsuits involving complaints about deep linking evidences sites' unwillingness to rely solely on technological solutions.

A site may also object to deep linking because it takes content out of context. The site may have been designed with a particular layout and intended viewing path. By coming in through a "side door" rather

[2]See, for example, *Computer Associates Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693 (2d Cir. 1992) (rejecting the *Whelan* case's holding and adopting a three-part test for separating unprotected ideas from copyright-protected expression).

[3]Parties set advertising rates in a number of ways. They may base the rate on the number of users seeing the ad, the number clicking-through to the sponsor's site, or the number clicking-through and purchasing something from the sponsor's site.

than the front, the deep linker sees the content out of order and in a way that might be misleading.

The deep-linking example illustrates how difficult it is to divorce questions of limiting access from defining the permissible means of access. Most sites would not argue that they can prevent another from employing a hyperlink to their home pages. It is the manner of accessing the site through a deep link to which they object.

In some of the most recent cases, the manner of access under attack is a bit less visible to the naked eye. Internet users have employed search engines throughout the medium's brief history as a commercial marketplace. Many search engines contain relatively limited content of their own. Instead, they use software programs called spiders or robots to crawl the Web, copying information about others' Web sites in the course of building their own databases. When a user enters a query, the engine searches its database and returns, minimally, the URLs (addresses) of sites likely to contain content of interest to the user. Historically, the indexed sites have had no reason to object to a spider's activities. Their revenue models almost always depended in some way on the number of visitors to their sites. Thus, the more travel to a site, the better—whatever the source, whether from a search engine, a link on another site, or the user's entering the URL into a Web browser directly.

AN UNTHINKING **TRANSPLANTATION OF TANGIBLE PROPERTY LAW** TO THE INTERNET IS LIKELY TO CREATE SOME UNDESIRABLE RESULTS.

But this "win-win" situation in which the indexed sites welcome search engines and users employ them as a primary means of locating information has begun to break down. Brands and brand names are establishing themselves on the Internet. The more powerful the brand, the more likely users will know its URL and travel directly to the site. An established site may prefer that users not access a search engine from which they may obtain information about competitive offerings and choose to visit another site.

Additionally, spiders, like all visitors to a site, impose a burden on the sites they visit, using system resources that would otherwise be free to process other requests, especially those from potential customers. At least theoretically, a large number of spiders crawling a site could cause the system to slow down or even crash. Either event can erode the site's goodwill with consumers and other paying customers. In the worst case, the performance degradation could drive a site out of business if it cannot either stop the spidering legally or technologically or afford to purchase (or legally compel the spider to purchase) additional capacity. In reality, however, the worst case scenario seems unlikely to occur. An individual spider likely imposes a minimal burden,[4] and Internet economics will not support an unlimited number of spiders. The advertising dollars many search engines depend on for their existence are limited, making it unlikely that a large number of spiders would both search and cripple a site.

In evaluating claims of unauthorized access, it is also difficult to ignore the eventual use of the information in which an unauthorized visitor might choose to engage. The visitor might wish to copy the visited site's information for personal or directly competitive purposes or as raw material in offering a new product. For example, one might copy eBay's product and pricing information as part of a research project on auction sites. One might copy it in the course of developing a directly competing auction site. A site like Bidder's Edge might copy it as part of the process of offering a new product, such as an index into auction sites that aggregates the search process. A user can go to Bidder's Edge, enter a search query, such as "Derek Jeter autographed baseball," and receive a list of all of the auction sites offering the item and their prices. Bidder's Edge is simply a specialized search engine. Other uses are likely to be in a gray area, potentially competing with the original site but also offering a new product that adds value to the original.

Intuitively, some of these uses offend less than others but all free-ride on eBay's content in some way. The question for policymakers is how to distinguish permissible from impermissible free-riding as a legal matter. The intertwined nature of the questions of access, legitimate means of access, and allowable uses of the information so obtained makes the legal response especially difficult to formulate.

Why Trespass Is an Attractive Analogy

Since time immemorial, common law courts have sustained a cause of action in trespass to real property.

[4] See, for example, *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1063 (N.D. Cal. 2000) (noting estimates that the Bidder's Edge spider used less than 2% of eBay's system capacity). The *eBay* court nevertheless preliminarily enjoined Bidder's Edge's use of a spider, holding that any unwanted access deprives *eBay* of some of its capacity, and that eBay could be damaged if many other firms began to use spiders to search its site. See id. at 1071-72. For a criticism of the *eBay* opinion, see *Bidder's Edge, Inc. v. eBay, Inc.*, No. 00-15995, Brief of Amici Curiae in Support of *Bidder's Edge, Inc.* , Appellant, Supporting Reversal (9th Cir. filed June 22, 2000).

Trespass to real property occurs whenever a person enters another's property without the owner's consent and without a legally recognized privilege that allows entry in the absence of such consent. It makes no difference whether or not the intrusion causes harm to the property or to its owner. Moreover, because the law recognizes few privileges, a landowner's rights in the U.S. in his or her property are close to inviolable.

Various rationales support this broad right to exclude. Landowners often have some financial and psychic attachment to their property, especially if they use it for personal rather than business purposes. A landowner may view any physical intrusion, however harmless, as threatening, and be tempted to respond with force and expend resources to keep out unwanted visitors. That intruders will be liable for trespass both deters their conduct and makes it less necessary for the landowner to resort to violence or to erect a barrier to entry.

Additionally, landowners are more likely to invest in improvements if they have a right to exclude others from entering their property and taking advantage of these improvements for free. A strong, certain right to exclude allows landowners to safeguard the value of their property by giving them the right to refuse entry, without conditioning that right on the construction of a fence that may be costly to build. This rule is further justified by other cost considerations. There are many would-be trespassers but usually only one or a few parties holding rights in the land, and the boundaries of the land itself are readily ascertainable. It is cheaper for those who wish to enter the land to approach the "well-known" landowner for permission than to require landowners to seek out and negotiate with those whom they cannot easily identify but want to exclude from entry.

Trespass to chattels applies the principles of trespass to land to personal property. It adjusts the real property cause of action to account for the differences between land and movable property. A person may be liable for trespass to chattels whenever he or she intentionally takes possession of another's chattel or causes a physical contact with or otherwise uses it. Unlike trespass to land, trespass to chattels requires the plaintiff to prove harm before being allowed to recover damages through a legal proceeding. The law justifies these differing rules by reference to the relative strength of the plaintiff's interest in the inviolability of his or her property. The law regards the attachment to land and interest in safeguarding it against intrusion as stronger than in the case of chattels.

Web sites are personal rather than real property. They are not land, and the servers on which they exist are generally freely portable. Also, the information a Web site contains is easily transferrable through the transmission of electronic signals. Therefore, the law on trespass to chattels that regulates the use of another's personal property seems an appropriate analogy in assessing claims of unauthorized access to Web sites. Visiting and using a Web site is the virtual analogy to touching and using a chattel.

In the 1990s, U.S. courts first applied trespass to chattels in the electronic context in cases involving spam (unsolicited bulk email).[5] Analogizing trespass to real property cases, they held the spam's electronic signals to be sufficiently tangible to interfere with the system receiving them. The legally cognizable harm arose not from damage to the chattel itself or a decline in its value, as in traditional cases, but from the impairment of the system's value. If it is occupied in processing spam, it cannot be processing other, desired communications. System providers may also suffer damage in the form of canceled subscriptions and expenditures to install technical measures to filter out spam. Additionally, consumers may be harmed because they incur costs in disposing of the unwanted email.

The analogy to conduct like deep linking and unauthorized spidering is straightforward. The entry through a "side door" by the deep linker and a spider's crawling are both unwanted virtual contacts with a Web site. The deep link causes damage by decreasing the linked site's revenue. Like spam, spidering decreases the system's availability for desired visitors. This performance slowdown may cost the site goodwill and, ultimately, revenue, because fewer visitors get to the site. To counteract performance degradation, the site may have no choice but to spend money to purchase more capacity or upgrade its filtering systems. An application of a trespass to chattels theory to address deep linking and spidering could be based on an analogy to the spam cases. Of course, spam cases are themselves based on an analogy to traditional, physical-world trespass to real property cases.

Why Trespass to Chattels May Not Be an Appropriate Cause of Action

Trespass to chattels seems, at least on the surface, to provide a workable analogy for the law to use in addressing claims of unauthorized access to Web sites. The differences between the physical and the virtual worlds, though, suggest that the law should develop a cause of action that takes into account the particular policy interests and characteristics of the Internet.[6]

Unlike land and chattels, a Web site is intangible

[5] See, for example, *Compuserve, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997).

property containing only information. The public interest in access to information on Web sites is likely to be greater than its interest in accessing another's land or chattels. There are First Amendment free-speech concerns that should be weighed before the law grants rights to control access to Web sites.[7] Trespass does not account for such interests.

Historically, copyright law has provided the set of rules governing exclusive rights in information, balancing these rights with the First Amendment rights of users. Notably, it has never accorded the copyright owner the exclusive right to control the manner in which a user views the copyrighted work. There is no law that prevents a person from starting a book in the middle, even though it might be misleading to take the material out of context in this way. There is also nothing to stop people from fast-forwarding past the commercials for which sponsors have paid when they watch a tape-recorded TV program. That the deep linker enters in the middle thus does not seem particularly troubling from a copyright perspective.

> THE QUESTION FOR POLICYMAKERS IS **HOW TO DISTINGUISH PERMISSIBLE FROM IMPERMISSIBLE FREE-RIDING** AS A LEGAL MATTER.

The copyright law has had less to say about access, leaving that question to other law. For example, a person might make "fair use" of a passage in a book. That this use would be permitted by copyright law does not entitle the person to break into a locked room to obtain a copy of the book. State law generally forbids this impermissible access. That the law respects a padlock—even one that protects access to information—in the real world suggests it should also do so in the virtual one. But publicly available Web sites are not locked in any sense, virtual or otherwise.

Indeed, Congress, in enacting the Digital Millennium Copyright Act in 1998, addressed the question of which access controls should be respected. Under the Act, "[n]o person shall circumvent a technological measure that effectively controls access to a [copyrighted] work."[8] A technological measure effectively controls access when it "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[9] The provision is intended to protect against hacking or cracking systems that require some form of digital key for entry. By inference, Congress is less concerned about circumvention of measures that do not provide digital information with as high a level of protection against intrusion. It would indeed be anomalous if state law on trespass to chattels were interpreted to prevent access to Web sites that federal law would allow. It would be particularly disturbing if trespass to chattels were to prevent access to uncopyrighted information when federal law (with which state law may not conflict) would permit access to copyrighted data.

The policy basis supporting trespass does not translate well into the virtual context. The physical separation between the actual entities conducting deep linking or spidering and the owner of a visited Web site renders the possibility of physical violence quite unlikely. The interest of Web site owners in the inviolability of their sites also seems significantly less than that of tangible property owners. The Internet has a tradition of open access to Web sites that have not deliberately erected a barrier to entry. A firm opts into this system merely through the act of placing its site on the Web.

A Modest Proposal

While trespass to chattels seems to have little to do with the policy interests or realities of the Internet, there are probably cases in which the law should allow a Web site owner to limit access. For example, the site's owner should usually be able to keep out those who have not paid the customary price. The owner should also be able legally to enjoin access conducted by means that place an unreasonable, unexpected burden on system resources. What is an "unreasonable" burden may vary depending on the facts but has yet to be implicated in actual litigation. A site should be able to stop copying and using its data when the copier is simply a pirate adding no new value. The key is to balance the incentive to create the initial Web site with incentives to develop new technologies like spiders and new products like the auction aggregator service offered by Bidder's Edge. Trespass does not allow this balancing.

A better test would be one that allows a court to consider a number of factors, including: the means

[6]For a deeper discussion of this topic, see Burk, D. The trouble with trespass. *J. Sm. Emerg. Bus. L.* 4 (2000), 27–56.

[7]A state law civil cause of action in trespass is unlikely to implicate First Amendment rights because the state's involvement does not rise to the level required to trigger constitutional protections. Nevertheless, the policy interests that the First Amendment represents should inform the design of property rights on the Web.

[8]17 U.S.C. ß 1201(a) (1999).

[9]Id.

and purpose of the access; the nature of the information taken; the burden the unwanted access places on the visited site; the effect of the access on the visited site's revenue; the cost to the visited site to gather the information it offers; and whether the access threatens the visited site's existence or quality. Such a test should also consider the public benefit that might reasonably be expected from allowing access to continue, as well as whether the visited site has taken technological measures to block access. The law should be more willing to enjoin unwanted access when the site has invested in technological measures like those protected under the Digital Millennium Copyright Act. Under such a test, a site like Bidder's Edge that offers consumers comparative pricing information without unduly burdening the eBay site would likely be allowed to continue its conduct. In contrast, a different site that copied information intending to offer it in direct competition with the visited site would often be enjoined.

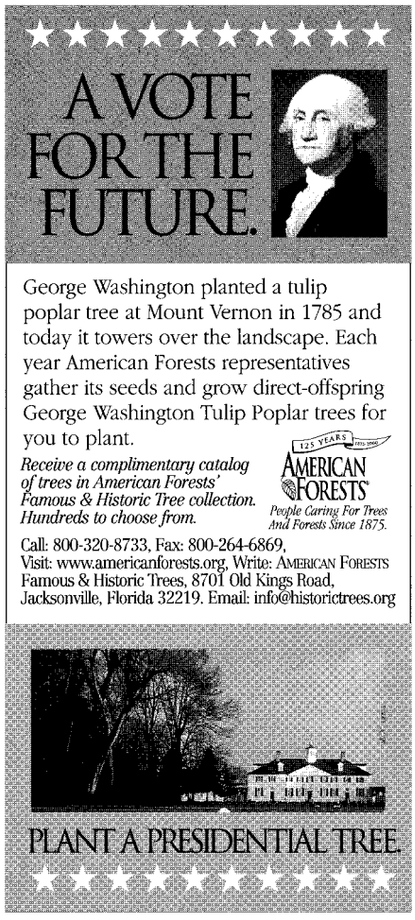
A balancing test like this creates some uncertainty, especially when compared to a bright-line rule that would allow all site owners to exclude whomever they want for whatever reason. Additionally, unlike a strong property right to exclude, such a test would tolerate a technological arms race until the site invests in measures protected under the Digital Millennium Copyright Act, and possibly beyond. However, at this relatively early stage of the Internet's development as a commercial marketplace, it may be appropriate to err on the side of weaker property rights that allow new, value-added technologies to flourish. The law may move to a regime of stronger rights over time, but, at least at the outset, weaker rights may enable a more vibrant network to develop.

Conclusion

The questions of who may access a Web site, how they may do so, and what they may do with the information they so obtain are not likely to go away. Courts today are facing pressure to apply law developed in the real world to the Internet by analogy. This approach risks obscuring the salient differences between the real and the virtual worlds. At this early stage of the technology, the more appropriate approach would be to follow the example of the software courts but to do so quickly—by recognizing these differences as the first claims arise and creating a new test appropriate to the Internet's special characteristics. C

Maureen A. O'Rourke (mo1@bu.edu) is a professor of law at Boston University School of Law.

© 2001 ACM 0002-0782/01/0200 $5.00





Toward a New Politics of Intellectual Property

PAMELA SAMUELSON

UNTIL recently, copyright was on the periphery of law because it involved technical rules for a highly specialized industry. The politics of copyright largely focused on intra-industry bickering. The typical response of a legislature to these intra-industry struggles has been to propose that affected parties meet behind closed doors and hammer out compromise language that would thereafter become law. It didn't matter much if the language negotiated in the heat of the night was incomprehensible (as has so often been the case) because the affected parties understood it, and that was all that mattered. Copyright law has, as a consequence, become highly complex and effectively unreadable.

Two important legacies of the old politics of intellectual property are these: First, copyright industry groups have cultivated relationships with policymakers in the executive and legislative branches over a long period of time. They have built up trust with these actors and they know how to get their messages across to these audiences effectively. Second, the public has gotten used to the idea that copyright doesn't concern them. It is, as a consequence, virtually impossible to mobilize the public when changes to copyright law are proposed.

Even though such changes will almost certainly have profound impacts on the public's use of information, they are so far from people's experience and expectations as to seem unreal. Even when some members of the public (such as USACM's public policy committee) do become engaged in the policy debates about copyright, they lack the political heft of industry counterparts, not the least because they will be less fruitful sources of campaign contributions.

Jack Valenti of the Motion Picture Association of America (MPAA) and Hilary Rosen of the Recording Industry Association of America (RIAA) have certainly not confided in me their plans for the next few sessions of Congress. However, from the many millions of dollars copyright industry organizations have poured into political campaigns in the past political season, it would be fair for them to believe they helped elect persons receptive to their concerns.

RIAA will surely be hoping to defeat the bill proposed by Rep. Boucher to permit the owners of music to listen to the music via services such as those operated briefly by MP3.com. If the Ninth Circuit Court of Appeals reverses the injunction against Napster, RIAA will also advocate legislation to overturn the decision. This might involve narrowing the "safe harbor" rules for ISPs (which the content industry always thought too generous to ISPs). It might also involve reconsideration of the Audio Home Recording Act if the court of appeals agrees with Napster that this law exempts noncommercial exchanges of digital music. The recording industry would like nothing better than to close this exemption and while Congress is at it, why not amend the provision that was too narrowly crafted to stop sales of devices such as the Rio player?

If the Secure Digital Music Initiative (SDMI) is being undermined by too much competition, it would be logical for the RIAA to ask Congress to mandate installation of SDMI technology to protect digital music. If this effort proved successful, a wider effort to mandate trusted systems would likely follow. The European Union has already raised the possibility of mandating trusted systems across the board in its copyright policy documents. The plain truth is that technical protection systems will never be truly safe until they are built into every part of the information infrastructure.

One reason to form a new politics of intellectual property is to counteract the content industry's drive toward ever-stronger rights. More importantly, a broader awareness is needed that copyright deeply affects the information environment for us all. The digital networked environment has surely changed the economics of production of intellectual property (for example, the marginal cost of copying is effectively zero), the economics of distribution (the cost of transmission via the Internet is also effectively zero), and the economics of publication (posting information on the Web is also

radically cheaper than in the print environment). This means, among other things, that the actions of individuals can have the same potential market-destructive impact as those of commercial counterfeiters in the olden days. This helps to explain why the content industries have been so anxious and why they favor moving to a pay-per-use or mandated trusted system policy for all commercially valuable information in digital form. Without imaginative proposals for more balanced solutions and without a political movement to support and sustain such proposals (in other words, without a new politics of intellectual property) there will be little to stop the current politics from having its high protectionist way.

James Boyle has argued for a new politics of intellectual property in his essay "Environmentalism for the Net." He points out that in the 1950s there was no concept of the natural environment. Logging and mining companies thought they alone were affected by legislation concerning natural resource issues and they lobbied for policies that sometimes caused erosion, pollution, and killed off wildlife. It took a while for society more generally to realize they had a common interest in the preservation of nature. They invented the concept of the environment that enabled a powerful political movement to protect it. Boyle hopes to ignite a similar movement to protect the intangible interests we all have in an open information environment, in robust public domain, and in balanced intellectual property law. It will sound strange perhaps to put it this way, but our information ecology really will be disrupted if intellectual property rights get too strong. So far Greenpeace hasn't taken up the cause, but maybe it should.

So who might participate in a new politics of intellectual property aimed at promoting a balanced information ecology? Obvious candidates include authors and artists (who need access to information, a robust public domain, and meaningful fair-use rights), educational institutions, libraries, scholarly societies, computing professionals groups, computer manufacturers and other equipment providers who don't want Hollywood to be in charge of their research and development divisions, telecommunications companies and Internet service and access providers (who want to serve their customers and not become a new branch of the police), economists, consumer groups, and digital media companies who may have some radical business models that just might work if not shut down through litigation by established copyright industry groups who want to protect preferred business models.

The agenda of a new politics of intellectual property obviously needs to be about more than just opposing the high protectionist initiatives of copyright industry groups. It needs to have a set of affirmative policy objectives of its own. Articulating a positive case for an open information environment is probably the single most important thing the new politics of intellectual property might do. The robustness and efficiency of the Internet as a communications medium is a product of its present end-to-end, open, nondiscriminatory architecture. Computers are not only more valuable to people because they can so quickly and easily copy information from disk to disk, but the ease of copying enables many beneficial new uses of information that copyright owners neither need to nor ought to be able to control. Innovation and competition would be stifled if mandated trusted systems became the law. Moreover, the market for digital information products may well be vastly smaller if every piece of information must be tightly locked up at all times. Branko Geravac once recommended that publishers "protect revenues, not bits." C

Articulating a positive case for an open information environment is probably the single most important thing the new politics of intellectual property might do.

Pamela Samuelson (pam@sims.berkeley.edu) is a professor of Information Management and of Law at the University of California at Berkeley.

Copyright held by author.

Pamela Samuelson

Does Information Really Have to be Licensed?

We have all purchased packaged software. After paying for it, we've taken the box home and loaded the software on our computer. We typically throw away the licensing agreement forms, although we may have glanced at them long enough to know these documents construe breaking open the plastic shrinkwrap or installing the software on a computer as assent to the terms of the license. These documents typically disclaim all warranties, tell you that some remote jurisdiction's law will apply in the event of a dispute over the software, and sometimes deny you authority to make backup copies, modify or resell the software, or decompile the code for any purpose. Most of us do not consider ourselves bound by these agreements because we never really agreed to them. If we go ahead and make backup copies or modify our copy of the software, we do so because it is a reasonable thing to do.

Up until now, the law has backed our reasonable expectations about packaged software distributed to the mass market. Most judicial opinions have refused to enforce shrinkwrap licenses because consumers have not meaningfully assented to the terms. They regard a contract of sale as having taken place at the time the store rings up the sale. The so-called license in the box, they say, may be a proposal to modify the nature of the transaction or add new terms, but consumers must separately agree to the revised contract and typically they don't.

From where, then, does the right of consumers to produce backup copies for possible resale if the original purchaser no longer needs it, decompile the program in order to fix a bug, or make an interoperable program come? It does not derive from pure reason alone; rather, its legal source is copyright law which has a longstanding tradition of balancing the interests of copyright owners and those of the consuming public. Although the states of Louisiana and Illinois once passed laws to validate software shrinkwrap licenses, neither statute survived closer review. In the *Vault vs. Quaid* decision, federal judges refused to enforce the Louisiana law insofar as license terms interfered with consumer rights under federal copyright law. The Illinois software shrinkwrap license enforcement

QUENTIN WEBB

IF UCC2B GAINS THE UNIVERSAL ADOPTION TO WHICH ITS PROPONENTS ASPIRE,

this model law may contribute to a fundamental transformation in the way information is disseminated in our culture, indeed, throughout the world.

statute was subsequently repealed due to industry dissatisfaction.

Factors Threatening the Status Quo

In the Internet era, the status quo on shrinkwrap licenses goes back practically to the Norman Conquest. (In England, the phrase "from time immemorial" expressed the concept of practically forever, the referent for which was the Norman Conquest in 1066.) Three factors currently threaten to upset this status quo.

The most significant factor is proposed Article 2B of the Uniform Commercial Code (UCC) about which I have written twice previously ("Legally Speaking," May and Oct. 1997). UCC2B is a model law designed for enactment by state legislatures. It would not only validate shrinkwrap and other mass-market licenses of information, it would also set rules about electronic contracting for information products and services, establish new rules about warranties, and allow software developers to embed "technical self-help" features that can be triggered if licensees fail to pay royalties for the software. Proponents hope to get approval of the draft at the July 1998 meeting of the National Conference of Commissioners on Uniform State Laws (NCCUSL), after which they expect state legislatures will begin considering its adoption. Previous UCC model laws, such as Article 2, which regulates sales of goods, and Article 2A, which regulates leases of goods, have been widely enacted by state legislatures with generally only minor variations (Louisiana once again being an exception).

Although the American Law Institute, the other body of lawyers to which UCC drafts are generally submitted for approval, has expressed serious reservations about UCC2B, this does not seem to have slowed down the NCCUSL process or the intention of proponents to seek fast legislative adoption of the model law.

While UCC2B is unquestionably the most important factor in the shifting environment about shrinkwrap licenses, two other factors deserve mention before we come back to a more in-depth discussion of UCC2B.

A second factor is a trend toward new distribution channels for software. Some companies have already started to distribute their software via the Internet. To purchase software this way, consumers have to click "I agree" to the thousand or more words' worth of contract terms they may view if they really care to before the downloading proceeds. This "click" will look to some judges like the meaningful assent to the license that has been missing from store-bought software. But consumers may still look to copyright policy as a legal basis for continuing to make reasonable uses of their software.

This brings us to the third factor which may change the status quo on shrinkwrap licenses: The 1996 *Pro-CD vs. Zeidenberg* decision.

Written by an influential appellate court judge, Frank Easterbrook, the decision enforced a shrinkwrap license restriction permitting only "home use" of a telephone directory on a CD-ROM. Judge Easterbrook not only ruled that the shrinkwrap restriction was enforceable as a matter of state contract law, but also rejected Zeidenberg's argument that posting of Pro-CD's telephone data on a Web site should be permitted because copyright policy favors the free flow of published information.

Judge Easterbrook offered three reasons why copyright policy should not override the shrinkwrap license restriction in that case. First, he observed that contract rights are different in nature and legal effect from such property rights as copyright. Contracts generally bind only the two parties who enter into the agreement, unlike property rights that generally are good against the world. Second, he asserted that the extra element of the user's agreement to the contract made the contract claim Pro-CD brought against Zeidenberg different from a copyright infringement claim. (The equiva-

lence of a copyright and contract claim would have led to the state law claim being preempted by federal copyright law and policy.) And third, Judge Easterbrook observed that Pro-CD would be unable to recoup its considerable investment in compiling, double-checking, formatting, and updating the telephone directory data if users could just upload the data onto their personal Web sites.

Naturally, the proponents of UCC2B are enthusiastic about the *Pro-CD vs. Zeidenberg* decision both for endorsing the idea that shrinkwrap restrictions can be enforced and for rejecting the copyright policy override argument. In that decision they see rather wishfully what they have believed all along.

But the *Pro-CD* ruling has not been without critics, especially in regards to its copyright policy analysis. Given the ubiquity of shrinkwrap licenses in the mass market for software and given the intent of licensors to bind the entire market, the commercial effect of enforcing these licenses would make them resemble property rights (that is, rights good against the world) more than contract rights (good only against the two parties to the contract). Moreover, it is a legal fiction to say that opening a package or installing software constitutes an agreement to the terms of a shrinkwrap license. Insofar as the act of unauthorized copying would necessarily underlie any contract or copyright claim in a case like *Pro-CD*, the two claims seem equivalent. This would seem to require preemption of the state contract claim by federal copyright law.

Some intellectual property scholars regard the only persuasive rationale for the *Pro-CD* decision to be that concerned with averting market failure, that is, with the effect of not enforcing the license on Pro-CD's ability to recoup its considerable investment in compiling this data and making it available to the public. This rationale supports a more limited interpretation of the *Pro-CD* decision. Under it, a court might enforce the "home use" restriction in *Pro-CD* because, as applied, it was a reasonable restriction and averted market failure. Yet, the same court could decide not to enforce restrictions on backup copying because Congress decided that backup copying was reasonable and doesn't threaten market failure.

Whatever one's view on the *Pro-CD* decision, it has unquestionably changed the intellectual landscape about shrinkwrap licenses and copyright policy. It gives a tremendous boost to the forces currently pushing for adoption of UCC2B. So let's take a closer look at UCC2B and what it says on these and related issues.

Dangers Lurking in UCC2B Licenses

The paradigmatic transaction of UCC2B is a license, that is, a limited transfer of rights to use information on stated terms and conditions. Contrast this with the dominant paradigm of the manufacturing age, namely, the sale of copies. Sales involve a complete transfer of ownership rights, in particular copies from the vendor to the purchaser, following which the purchaser could largely do whatever he or she wished. If you own a copy of a copyrighted work, you can sell or give it away to friends. However, you can generally redistribute a licensed copy only if you have specially contracted for the right to do this. If UCC2B gains the universal adoption to which its proponents aspire, this model law may contribute to a fundamental transformation in the way information is disseminated in our culture, indeed, throughout the world. UCC2B may herald the shrinkwrapping of information of all kinds—books, magazines, CDs, movies—you name it.

The problem is that UCC2B would validate mass market as well as negotiated licenses for information as long as a consumer has manifested token assent to the license by such acts as clicking "I agree" or loading the information onto a computer after an opportunity to review the often lengthy and sometimes incomprehensible terms of the license.

Only if the terms of a license are "unconscionable" (shockingly oppressive) will UCC2B refuse to enforce them. Proponents seem to think that UCC2B should be permissible to waive all of the default rules of copyright law, such as the right to make backup copies, in mass market as well as in negotiated licenses. UCC2B is structured to ensure that this occurs.

Suppose, for example, Microsoft decided it didn't want you to make fair uses of its software when you acquired one of its products. Microsoft should be free, so the theory goes, to offer you software on terms that call

UCC2B MAY HERALD THE SHRINKWRAPPING OF INFORMATION OF

all kinds—books, magazines, CDs, movies—you name it.

upon you to waive this right.

Microsoft argues that this promotes freedom of contract and that competition can be counted on to ensure that information providers will be responsive to consumer demands. If consumers find such terms unacceptable, they'll decide not to license information from certain vendors. If enough consumers believe the same, the market will, in theory, correct the imbalance. (Of course, the theory doesn't work if the market is dominated by one firm or a small number of firms adopting the same onerous licensing terms.)

One of Microsoft's licensing officials, Robert Gomulkiewicz, has put the new paradigm of UCC2B succinctly: "The product is the license." (Think how weird it sounds to say, "let's go and shop for some licenses.")

In the new world order of UCC2B, you get what you pay for. But all you may get is a license with highly restrictive terms, any breach of which terminates any rights you have under the license. One minute you're a licensee; the next minute you're an outlaw. If information ever wanted to be free, it must have changed its mind because under UCC2B, information seems intent on being licensed.

Incidentally, in case you have any doubts about what people at Microsoft think about fair use, let me relate this story: While working at Microsoft during the summer of 1997, one of my students went to the annual summer intern hot-dog party at which Bill Gates invited questions from the interns. My student asked Gates what he thought about fair use. Gates laughed. And then he said: "You don't need fair use; we'll give you fair-use rights when you need them." (That's what's got some of us worried, Bill.)

The Clash Between UCC2B and Intellectual Property Policy

Intellectual property professionals who have studied the proposed UCC2B have challenged the notion that software developers (or any other information provider) can unilaterally bypass public policy limitations imposed by copyright law by adopting restrictive mass-market licenses.

At a conference hosted by the Berkeley Center for Law and Technology at the University of California at Berkeley, copyright scholar David Nimmer pointed out that computer software firms are far from the first information providers to attempt to use restrictive licensing agreements to control mass-market distributions of their products.

Book publishers and sound-recording companies once tried to restrict what purchasers could do with their products by licenses, but fortunately the courts didn't let them get away with it. (Take a look at an old Victrola recording jacket and you'll see it purports to license use of the recording to one Victrola machine and to deny authority to retransfer one's copy of the recording.)

One important case was *Bobbs-Merrill vs. Straus*. Publisher Bobbs-Merrill sued Straus, a bookseller, because he sold copies of Bobbs-Merrill books in violation of a license restriction that conditioned the right to retransfer copies of the books on an agreement to charge at least $1 per copy. The U.S. Supreme Court treated the license restriction as ineffective as a matter of copyright policy. The *Bobbs-Merrill* decision contributed to the emergence of the "first-sale" or "exhaustion-of-rights" doctrine in copyright law, under which publishers lose authority to control redistributions of copies of their works when, in commercial reality, the transaction is a sale. In the aftermath of this and similar cases, publishers and sound-recording companies abandoned these practices.

While explanatory notes to UCC2B say the article will not affect the sale of books and newspapers, they do not cite to *Bobbs-Merrill*. Nor do they indicate that publishers or sound-recording companies should not expect success if they attempt to displace copyright's first-sale doctrine by means of mass-market shrinkwrap license restrictions.

Because UCC2B presumes licenses of all sorts are enforceable, it is reasonable to interpret the draft as intending to provide print publishers with the same freedom of contract provided to software developers. Yet, many copyright professionals would

strongly disagree with that result and believe that this should not be the end of the matter.

Copyright Preemption

The U.S. Constitution provides that when a state law rule conflicts with federal law or policy, federal law will be supreme. If, for example, a state rule would allow an exclusive license of a copyrighted work to be created by an exchange of words, federal copyright law would preempt the state rule because federal copyright law requires a signed writing before an exclusive license could be enforced. One of the most contentious issues about UCC2B is whether federal copyright policy will preempt enforcement of mass-market licensing terms waiving fair use or similar rights.

The drafters proposed UCC2B recognize the potential for conflicts between its provisions and federal intellectual property law. Section 2B-105 says that "[a] provision of this article which is preempted by federal law is unenforceable to the extent of such preemption." The current draft of UCC2B claims it is neutral on the issue of preemption, seeming to leave to litigation the ultimate determination of the contours of preemption. In a paper prepared for the Berkeley conference on the intersection of intellectual property policy and UCC2B, Ray Nimmer (who is no relation to David Nimmer, mentioned earlier), the principal drafter for the UCC2B project, demonstrates that he's not neutral on the subject of preemption. Ray Nimmer's report states there are no circumstances in which UCC2B or any license governed by it might be preempted.

Even when federal copyright law has explicitly made a certain right of authors nonwaivable by contract, Ray Nimmer thinks it can be avoided by a 2B license of perpetual duration. Copyright professionals would contest this conclusion.

On the more general issue of copyright preemption of terms of contracts, it is useful to compare the two Nimmer articles [1, 2]. David, the copyright specialist, offers many examples of contract terms in copyright licenses that are likely to be preempted. It remains to be seen whose prediction about preemption will be borne out, but my bet is on David.

Leery of leaving the preemption issue entirely to litigation—partly because litigation is such a time-consuming and expensive process and partly because state courts do not have much experience ruling on copyright policy matters in view of the exclusive jurisdiction Congress has conferred on federal courts in copyright cases some have sought a more direct way to resolve the copyright preemption issue presented by UCC2B mass-market licenses. At the American Law Institute meeting in May 1997, Charles McManis, a copyright expert, made a motion to amend the mass-market license provision of UCC2B to clarify that these licenses can't override fair use and other user rights under specified provisions of federal copyright law. This motion passed at the ALI meeting. But at a subsequent NCCUSL meeting, after heavy lobbying by information industry groups, a counter motion passed asking the ALI to reconsider the McManis motion.

Meanwhile, in Congress, Representatives Rick Boucher (D-Va.) and Tom Campbell (R-Ca.) have included a provision very similar to the McManis motion in H.R. 3048 (the good copyright bill before Congress this year). But despite having 40 or more sponsors, the Campbell-Boucher bill has not achieved the momentum of a rival bill, H.R. 2281, which major copyright industry groups and the Clinton administration favor. H.R. 2281 contains no provision on preemption of mass-market license terms. So it looks like litigation will be the way that the great preemption debate posed by Nimmer vs. Nimmer will be resolved.

Conclusion

There are a host of reasons why UCC2B should not be adopted in its present form. Many of these, as well as many pro-UCC2B statements, can be found on the Web site maintained by Carol Kunze at www.softwareindustry.org/issues/guide.

The ALI has insisted that substantial changes be made to the draft before it will consider endorsing the model law. A few changes have already been made to respond to the ALI concerns, but much work remains to be done.

At the Berkeley conference on UCC2B, Michael Froomkin, a law professor from the University of Miami, likened UCC2B to a beta version of a huge new operating system program on the account of its breadth, complexity, and many novel provisions (including one that would

COMMUNICATIONS OF THE ACM
November 1998

Special Section:
High Performance Computing

architecture
digital libraries
programming tools
education
training
metasystems

Also In This Issue:
software engineering
programming
internet

Bonus Distribution:
Supercomputing
Orlando, FL

Display Advertising Closes:
September 28, 1998

For more information contact:

ACM Advertising
212-626-0685
acm-advertising@acm

enforce contracts formed by "reasonably configured" electronic agents). Is it really a good idea to trust the health and vitality of our emerging information economy to such an untested beast?

While one can admire the grand ambition underlying the UCC2B effort to anticipate and engrave in legal stone a complex set of rules for the global information economy, one can also question whether it is really possible to get it right at this point in time. Wouldn't it be better to start more modestly with a few key provisions that may be needed to get electronic commerce off the ground, and then revisit the rules periodically to conform them to the electronic and information commerce that achieves market success? Commercial law rules, said contracts scholar Grant Gilmore, should be "accurate, not original." UCC2B violates this maxim in a number of respects.

Unfortunately, state legislatures are far too likely to assume the years that have gone into the development of UCC2B must mean it has produced a very good product. They may also fall for slick arguments by lobbyists for information industry groups that support it (not all do, by the way) who may assert that the state's early adoption of UCC2B will cause information businesses from all over to flock to that state. This is the sucker tactic that apparently persuaded the Louisiana legislature in the early 1980s to pass the shrinkwrap license enforcement statute that the *Vault vs. Quaid* case refused to enforce because of its conflict with federal copyright policy.

If these tactics worked once, they may work again. Why else would the legislatures of Wisconsin and Iowa supposedly be champing at the bit to enact UCC2B, as proponents of the model law claimed at the Berkeley conference?

The debate about copyright preemption of shrinkwrap license terms boils down to whether copyright owners can have their cake and eat it too. Copyright law has always (and wisely) insisted on there being a balance between the rights conferred on authors and the rights reserved to the public. The balance has been key to ensuring that copyright law fulfills its constitutional mandate of "promot[ing] the progress of science and [the] useful arts."

Lately that balance has been under assault, as high protectionists have sought overbroad copyright legislation, new forms of legal protection against extractions of information from databases, and now mass-market licenses capable of overriding the public policy balances of copyright law. We shouldn't let them get away with it. If publishers want the rights that copyright confers, they must take the responsibilities along with the rights. C

References

1. Nimmer, D., Brown, E., and Frischling, G.N. The metamorphosis of contract into expand,. *Calif. L. Rev.* (forthcoming, 1998).
2. Nimmer, R. Breaking barriers: The relation of contract and intellectual property law. *Berkeley Techn. L.J.* (forthcoming, 1998).

Pamela Samuelson (pam@sims.berkeley.edu) is a professor of Information Management and of Law at the University of California, Berkeley, and co-director of the Berkeley Center for Law and Technology.

© 1998 ACM 0002-0782/98/0900 $5.00

[The following article appeared in the January 1996 edition of Wired]
[http://www.wired.com/wired/archive/4.01/white.paper_pr.html]

The Copyright Grab

The Clinton administration, through its white paper on intellectual property, is proposing a wholesale giveaway to its supporters in the copyright industry - at your expense.

By Pamela Samuelson

Browsing through a borrowed book, lending a magazine to a friend, copying a news article for your files - all seem innocuous enough. But the Clinton administration plans to make such activities illegal for works distributed via digital networks. If legislation recommended in its white paper "Intellectual Property and the National Information Infrastructure" is enacted, your traditional user rights to browse, share, or make private noncommercial copies of copyrighted works will be rescinded. Not only that, your online service provider will be forced to snoop through your files, ready to cut you off and turn you in if it finds any unlicensed material there. The white paper regards digital technology as so threatening to the future of the publishing industry that the public must be stripped of all the rights copyright law has long recognized - including the rights of privacy. Vice President Al Gore has promised that the National Information Infrastructure (NII) will dramatically enhance public access to information; now we find out that it will be available only on a pay-per-use basis.

Why would the Clinton administration want to transform the emerging information superhighway into a publisher-dominated toll road? The most plausible explanation is a simple one: campaign contributions. The administration wants to please the copyright industry, especially members of the Hollywood community, who are vital to the president's reelection bid. And what this copyright industry wants in return is more legal control than ever before over the products they distribute.

The US Constitution empowers Congress to pass laws "to promote progress of science and [the] useful arts." Congress has chosen to accomplish this constitutional goal by granting authors a limited set of exclusive rights in their works. Copyright protects all original works of authorship, including such things as personal letters and corporate memoranda, from the moment they are first fixed in a tangible form. This protection attaches automatically by operation of law and lasts for the life of the author plus 50 years. In the three centuries of its existence, copyright law has focused on regulating public and commercial activities, such as the commercial reproduction of physical objects embodying the copyrighted work (books, for example) for intended dissemination to the public, the commercial distribution of physical copies to the public, and public performances of dramas, music, and the like. (Singing a copyrighted tune in the shower is not an infringement because it is a private performance of the music.)

Some publishers, however, want to control not only all public and commercial uses of their works, but all private uses as well. They assert that this would better fulfill the constitutional purpose of copyright, because the greater the financial return to them, the greater will be their incentive to make works available to the public. Proponents of this view suffered a setback in 1984, when the Supreme Court ruled in the Sony

Betamax case that taping a television program for time-shifting purposes in the privacy of one's own home was "fair use" (and consequently that Sony wasn't liable to Universal and Disney for contributory copyright infringement in selling videotape machines). But these publishers fear digital technology far more than videotape machines. Ever since they began to realize that digital technologies could "free" information dissemination, the established copyright industry has been shaking in its boots. Now a group of major motion picture producers, sound recording companies, and print publishers have figured out a way to turn the threat of digital technology into an opportunity. Under this plan, they would retain all of their rights under existing law and quietly attain a host of new ones.

Bruce Lehman, Clinton's czar of intellectual property policy and the person in charge of shepherding the white paper's NII Copyright Protection Act through Congress, is, coincidentally enough, a former copyright industry lobbyist. Lehman - whose official titles are assistant secretary of commerce, commissioner of patents and trademarks, and chair of the Intellectual Property Working Group of the administration's NII task force - depicts the changes to copyright law recommended in the white paper as minor clarifications and updates to existing law. They are, in fact, a flagrant giveaway to the copyright industry, softened only by two public-interest provisions added to make the package appear more balanced than it really is. (One provision would expand library privileges to make copies of copyrighted works for archival purposes, and the other would permit nonprofit groups to distribute Braille or large-type editions of copyrighted works if the publisher has neglected to do so within a year of publication of the standard edition of the work.)

Bipartisan bills to implement the white paper proposals were introduced in the House (HR 2441) and the Senate (S 1284) in late September. Lehman and the copyright maximalists are relying on several factors to get this legislation through Congress before the public realizes what is happening and rouses itself to action. First, Congress finds it difficult to say no to copyright producers, who are not only often glamorous but make a positive contribution to the US balance of trade (US$45.8 billion in 1993). Second, many influential members of Congress know and trust Lehman, who was a Congressional staffer before he became a copyright lobbyist. Third, copyright has become such a complex and esoteric law that many senators and representatives, as well as members of the press, will not be able to penetrate the 250-page, jargon-ridden white paper to learn that there is good reason to be skeptical about it.

Quick Congressional acceptance of the white paper's legislative package will help persuade courts to accept the white paper's interpretations of existing law as a kind of legislative history of the NII Copyright Protection Act. Thus, if the Clinton administration's legislative proposal is adopted, the maximalists may finally get the law they have always wanted instead of the more limited grant of rights that the Constitution has long been understood to authorize.

The maximalist agenda

The eight interrelated parts of the white paper's agenda intend to:

1. Give copyright owners control over every use of copyrighted works in digital form by interpreting existing law as being violated whenever users make even temporary

reproductions of works in the random access memory of their computers;

2. Give copyright owners control over every transmission of works in digital form by amending the copyright statute so that digital transmissions will be regarded as distributions of copies to the public;

3. Eliminate fair-use rights whenever a use might be licensed. (The copyright maximalists assert that there is no piece of a copyrighted work small enough that they are uninterested in charging for its use, and no use private enough that they aren't willing to track it down and charge for it. In this vision of the future, a user who has copied even a paragraph from an electronic journal to share with a friend will be as much a criminal as the person who tampers with an electrical meter at a friend's house in order to siphon off free electricity. If a few users have to go to jail for copyright offenses, well, that's a small price to pay to ensure that the population learns new patterns of behavior in the digital age.);

4. Deprive the public of the "first sale" rights it has long enjoyed in the print world (the rights that permit you to redistribute your own copy of a work after the publisher's first sale of it to you), because the white paper treats electronic forwarding as a violation of both the reproduction and distribution rights of copyright law;

5. Attach copyright management information to digital copies of a work, ensuring that publishers can track every use made of digital copies and trace where each copy resides on the network and what is being done with it at any time;

6. Protect every digital copy of every work technologically (by encryption, for example) and make illegal any attempt to circumvent that protection;

7. Force online service providers to become copyright police, charged with implementing pay-per-use rules. (These providers will be responsible not only for cutting off service to scofflaws but also for reporting copyright crime to the criminal justice authorities);

8. Teach the new copyright rules of the road to children throughout their years at school.

It's hard to fully appreciate how substantial a change the white paper would wreak upon copyright law until you grasp the negative synergies among its eight interrelated parts. The diminishment of fair-use rights, for example, might seem less threatening when viewed in isolation than when viewed in conjunction with the white paper's call for an expansion of copyright owner control over browsing and transmissions.

The copyright maximalists are also hoping that quick adoption of the white paper's legislative proposals will be a steppingstone to international adoption of their agenda. Bruce Lehman has already attended several international meetings advocating the Clinton administration's copyright package as the right set of rules for the Global Information Infrastructure (GII). At meetings sponsored by the World Intellectual Property Organization, Lehman has urged that the white paper's legislative proposals be included in a supplementary agreement (known as a protocol) to the major international treaty on copyright matters, the Berne Convention. Since participation in

the organization's meetings is limited to intellectual property professionals associated with special interest groups or governmental organizations (many of whom, like Lehman, are now in policy making positions in their governments), the chances for the maximalists to gain international acceptance of their agenda - at least by governments, if not by the people they purport to represent - seem strong. If they succeed, member countries would be substantially constrained by treaty obligations from later amending their national laws to make them less restrictive about information dissemination. So, if the public ultimately were to decide the maximalists' agenda is unacceptable, a whole new treaty would have to be negotiated to undo the damage. That would take years, if it could be done at all, and naturally the maximalists would fight it every step of the way.

The white paper seeks to implement the maximalist agenda partly by rewriting the copyright statute and partly by aggressively interpreting existing law. Legislatively, it seeks 1) an amendment to treat digital transmissions of works as distributions of copies to the public; 2) a new provision making it unlawful to tamper with copyright management information; and 3) a new provision to prohibit devices or services aimed at circumventing technological protection for copyrighted works. To implement the rest of the agenda, it relies on the old litigation trick of acting as though the law is already firmly on your side. Although the white paper purports to be an objective statement of existing law, it is really a skillful advocacy document; on virtually every controversial issue of the day, it takes the maximalist view, often without acknowledging that contrary arguments or authority even exist. Where existing case law does not conform to the maximalist view, the white paper simply ignores it. This bias is glaringly evident when one closely examines the eight major issues:

1. The exclusive right to read: The white paper seeks to extend publisher rights to control browsing and other uses of copyrighted works in digital form by an expansive interpretation of existing law. It observes that in order to browse a digital work, the user's computer must make a temporary copy of that work in its random access memory; that temporary copy, it claims, is an infringing reproduction of the work unless it has been licensed or is otherwise privileged. The white paper relies on an appellate court decision that treated the unlicensed loading of a computer program in RAM as an infringing reproduction. But it knowingly omits reference to the legislative history of the current copyright statute, in which Congress specifically stated that the temporary storage of a copyrighted work in a computer's memory should not be regarded as an infringing reproduction. Rather than seek legislative clarification on this issue, the white paper simply pretends that under existing law, browsing is an infringement, hoping thereby to avoid tough questions from senators and representatives whose constituents might be worried about granting copyright owners an exclusive right to control all readings of works in digital form.

2. The exclusive right to transmit: Lehman has been leading the drive for adoption of the white paper's proposed NII Copyright Protection Act on the theory that it is unclear under existing law whether a digital transmission is a distribution of a copy to the public. The act, he says, will make clear that this is so. But the white paper admits that the courts have already regarded digital transmissions of copyrighted works as infringing distributions in some cases, so either there is an unstated purpose behind this proposal, or else it is just a smoke screen to deflect attention from the real kickers in the package. Lehman is probably seeking the digital transmission amendments

because his pals among the maximalists want to be able to control all performances and displays of copyrighted works, not just the public performances and public displays that the existing law grants to copyright owners.

3. The end of fair-use rights: The white paper attempts to eliminate fair-use rights by interpreting existing law as though fair use has no application when a use can be licensed (remember that the maximalists believe all uses can be licensed). Copyright maximalists, in fact, regard all unauthorized copying of copyrighted work as theft. This theory has, however, been rejected by the US Supreme Court. Universal and Disney once sued Sony to stop distribution of its videotape machines, arguing that private noncommercial copying of their motion pictures by purchasers of Betamax machines was no more excusable than the theft of a necklace because the thief intended to wear it only at home for noncommercial purposes. The Supreme Court pointed out that the person who steals a necklace deprives its owner of possession and use of the item, whereas the copying of programs off the air "does not even remotely entail comparable consequences for the copyright owner." The Court held that it was fair use for consumers to copy programs off the air for time-shifting purposes. Indeed, the Court said that private, noncommercial copying should be presumed fair use.

The white paper makes no mention of this aspect of the Sony ruling. It reinterprets the case as though the Court found no infringement because Universal and Walt Disney had not yet established a licensing market for off-the-air copying of their works.

The notion that fair-use rights apply only when no licensing market exists is neither historically accurate nor good public policy. It ignores some important free speech and related public interest functions of fair use that were recognized in cases such as Time Inc. v. Geis. Time sued Bernard Geis for copyright infringement because he included in his book about the Kennedy assassination sketches of frames from the Zapruder film (whose copyright Time had acquired) to illustrate his rationale for concluding that Lee Harvey Oswald was not the sole gunman. Time lost this lawsuit - not because it had no pricing schedule by which Geis could have licensed the right to reproduce the frames, but because allowing Geis to use the frames in his book was consistent with the constitutional purposes of copyright to promote knowledge, public access to knowledge, and public discourse about this important event. The same rationale explains why senators and representatives read newspaper articles into the Congressional Record to preserve their importance to public debate on controversial issues, and why many of us share copies of articles with people we know are concerned about particular issues.

Another case illustrating the broader public policy purposes of fair use is Sega v. Accolade. (The white paper also ignores this case.) Accolade decided not to pay license fees to Sega in order to get access to information about how to make its videogames run in Sega Genesis machines. Instead, it decompiled the Sega code, extracted the interface information, and then wrote program code to reimplement the interface so that Accolade's cartridges would run in the Sega machines. Sega charged Accolade with copyright infringement arising from its decompilation efforts. A federal appellate court decided that Accolade's intermediate copying of the Sega program for a legitimate purpose, such as getting access to the functional requirements for achieving compatibility, was a fair use. The court thought that ruling in Sega's favor would have undermined copyright principles by giving Sega a broader monopoly over the contents

of its program than Congress intended. In contrast, ruling in Accolade's favor was consistent with the constitutional purposes of copyright to promote the creation and distribution of new no infringing works.

4. Eliminating first-sale rights for digitally transmitted documents: Copyright owners have historically been entitled to control only the first sale of copies of a work to the public. After that, the consumer who has bought the copy can share it with a friend, give it away, or resell it. (Libraries rely on first-sale rights to lend copies of books to the public.) Consumers would expect the same rule to apply if the copy was electronic. But the white paper says that sharing your copy of an electronic work with a friend is illegal because, in order to send that copy to your friend, your computer will have to make a copy of the document; and since that copy hasn't been authorized by the copyright owner, an infringing reproduction of the work has taken place. If the white paper had wanted to retain the balance of interests embodied in current law, it would have suggested that the intermediate copying necessary to effect a user's first-sale rights should be regarded as a fair use under precedents such as Sega v. Accolade.

5. Helping documents spy on you: The white paper anticipates that publishers will want to attach copyright management information to digital forms of their works. It defines copyright management information as "the name and other identifying information of the author of a work, the name and other identifying information of the copyright owner, terms and conditions for uses of the work, and such other information as the Register of Copyrights may prescribe by regulation." It proposes to protect this information against tampering by making it illegal to knowingly remove or alter copyright management information or to distribute copies of works whose information has been tampered with. Money damages and criminal penalties would await violators.

While one can question whether it's necessary to make tampering with copyright management information a crime (much less a felony), this provision seems relatively innocuous at first blush. I didn't start worrying about it until I heard proponents talking about how copyright management information systems might be implemented. Some favor making these systems "dumb," while others favor making them "smart." Dumb systems would simply identify the work with a digital equivalent of the ISBN numbers used in the book world today. Smart ones would, among other things, have the ability to secretly report back to the copyright owner via the network on what the user was doing with the work, and the ability to search the consumer's hard disk and report back on what else was there. The Microsoft registration wizard may be just the beginning of the intrusive snooping to which copyright owners will be prone - only, in the future, it won't be possible to say no, and any effort you make to block these intrusions may make you a felon.

Plans are also underway to develop secure processors that won't permit copying of digital works unless their copyright management information authorizes it. Some publishers are already talking about getting governments to mandate inclusion of these secure processors in all reprography technologies (including photocopy machines). The precedent they offer for this mandate is the serial copy management system requirement imposed on manufacturers of digital audio-tape machines. They conveniently forget that the law regulating these machines does not ban all unauthorized copying; it permits consumers to make first-generation copies but not multiple secondary reproductions identical in quality to the digital material from which

they are derived.

There is very little in the white paper to inform Congress or the public about these additional plans for copyright management information. It's also worth noting that the white paper never contemplates a situation in which a user might have a legitimate reason to alter copyright management information or to defeat technological protection. It seems to assume that consumers of information products are would-be thieves and that content owners are just trying to make an honest living.

6. Outlawing decryption: Many copyright owners are planning to protect digital forms of their products by technological means such as encryption. To ensure the security of this technological protection, the white paper recommends the following legislation: "No person shall import, manufacture, or distribute any device, product or component incorporated into a device or product, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism, or system which prevents or inhibits the violation of any of the exclusive rights of the copyright owner under section 106."

Civil penalties for violation of this law will include having to pay statutorily established damages and having any equipment used in the process (your computer, for example) impounded. While one can understand the desire to prevent decryption for the purposes of redistribution and profit, the provision doesn't require either of these as a precondition for liability. Merely manufacturing or distributing a technology that can be used to undo a system that a copyright owner has adopted to protect its work seems sufficient to incur liability.

Although the white paper doesn't say so, this legislation would overturn a second ruling in the Supreme Court's Sony Betamax decision, which held that copyright owners cannot stop distribution of a technology as long as it has a substantial noninfringing use.

In addition, the language of this proposed law is so broad and so vague that it can be construed as outlawing many activities widely believed to be lawful. For example, some software publishers will argue that the decompilation of mass-marketed software in order to get access to interface information violates this provision, because the decompiler would be performing a service whose primary purpose and effect was to bypass the technological system the program's developer had adopted to protect its program (distribution of the program in object code form in order to maintain the contents of the program as a trade secret). Although Sega v. Accolade and another federal appellate court decision have affirmed the right of software developers to decompile software for compatibility purposes, the white paper doesn't mention the decompilation and interoperability case law. Lehman and the maximalist software publishers who used to be his clients insist that decompilation is and should be illegal. They are hoping to overturn the decompilation case law indirectly by the white paper's endorsement of some changes to commercial law that would validate common terms in shrink-wrap licenses, such as prohibitions on decompilation.

What the white paper doesn't mention is that previous industry attempts to protect copyrighted works in digital form by technological means failed in the marketplace as

well as the courts. Users, who often felt there were legitimate reasons for them to have access to an unrestricted version of a program, created a demand for programs that could defeat software copy-protection systems. Litigation soon ensued. Vault, whose copy-protection software could be defeated through use of Quaid's unlocking program, sued Quaid to try to stop distribution of the latter's software. Vault relied in part on a Louisiana law intended to validate common terms of software shrink-wrap licenses. But because Quaid's software allowed purchasers of application programs to exercise rights conferred on them by copyright law to make backup copies and modifications to the software, the court decided that what Quaid had done was lawful. To the extent that the Louisiana law might stop users from exercising their rights under copyright law, the court decided the state law conflicted with the purposes of federal law and was unenforceable. The message of the marketplace was equally clear: Software developers eventually abandoned the distribution of copy-protected software because it was unpopular with consumers. Even though the market for locking and unlocking software died out - making it easy to copy software in digital form - the software industry as a whole has thrived.

7. Turning online service providers into cops: The white paper asserts that every online service provider is already liable for all copyright infringement committed by its users, regardless of whether the service has reason to know about the infringement or takes reasonable steps to ensure that it won't occur. To back up this view, the white paper cites two lines of cases.

In one set, employers were found vicariously liable for copyright infringement by their employees when they had the power to supervise their employees' activities and financially benefited from the infringement. In the second set of cases, nightclub owners were held liable for infringements by bands they had warned not to perform copyrighted music without a license, because the owners had rights to supervise the bands and because they benefited from the infringement.

There is, however, other case law that goes unmentioned in the white paper which supports the online service providers' contentions that they should not be held strictly liable for user infringements. Landlords, for example, have escaped liability for infringements committed by their tenants because they had very limited power to inspect the infringers' premises or supervise their activities, and because they didn't financially benefit from the tenants' infringement. Online service providers liken themselves to landlords because they typically "rent" space on their computers to users who store private material, such as e-mail, there. Also, they typically do not monitor user activities (except for automated searches for certain profane words or screening for threatening language). Indeed, they are forbidden by the Electronic Communications Privacy Act from monitoring the content of private user messages, another factor the white paper ignores in the balancing equation. They also argue that they don't b nefit financially from user infringements.

Some commentators have argued that imposing a strict liability rule on online service providers is inconsistent with the public policy purposes underlying copyright law because it will chill so many noninfringing online exchanges of information. If online service providers have to monitor everything users do, they will artificially impose centralized structures of control over user communications. The danger that overzealous copyright owners will sue online service providers in order to censor online

communications has already evidenced itself in the ongoing Religious Technology Center and Bridge Publications Inc. v. Netcom case. (The copyright holder and publisher, respectively, of Church of Scientology materials have sued Netcom and a church dissident for copyright and trade secret violations because the dissident used his Netcom account to post church teachings. See Wired 3.12, page 172.)

The white paper is quite frank in its determination that online service providers should become centralized control centers to enforce copyright law. "They - and perhaps only they - are in a position to know the identity and activities of their subscribers and to stop unlawful activities. And, although indemnification from their subscribers may not reimburse them to the full extent of their liability and other measures may add to their costs of doing business, they are still in a better position to prevent or stop infringement than the copyright owner. Between these two relatively innocent parties, the best policy is to hold the service provider liable." This statement, however, ignores the privacy interests of users, as well as serious questions about whether it is technically feasible for online services with millions of subscribers to do the continuous monitoring of user accounts that copyright owners might like. The white paper acts as though the interests of copyright owners so override other, competing interests that it isn't even worth mentioning what the other interests are, let alone trying to balance them against the copyright owner interests.

8. Teaching children not to share: To ensure that future generations are broken of the habit of thinking that it's OK to share copies of copyrighted works with a friend, the white paper offers examples of lessons about copyright that could be taught as early as kindergarten and as late as college. The general theme of these lessons, in order not to be\ too negative, would be, "Just say yes" to licensing. (It actually says this.)

Reasons to say no to the white paper's agenda

When Bruce Lehman talks to the public about the white paper, he acts as though unless copyright law is strengthened, no content will be available on the NII, because publishers won't have the incentive to provide it. The white paper seems oblivious to the phenomenal growth of the World Wide Web and other areas on the Internet where a wide variety of content is already available. In the few places where the white paper acknowledges the existence of the Net culture, it is overtly hostile to it, characterizing it as a "legal free-for all [that] would transform the GII into a veritable copyright Dodge City." Lehman aims to be the sheriff who will kick those anarchic digital cowboys off the Net and make the electronic frontier safe for businesses that want to set up shop there.

Lehman also likes to invoke for the public a utopian vision of ubiquitous and cheap availability of content on the NII if the public accepts his proposed changes to copyright law. If people will only pay for each access to a work, he implies, content owners will make their intellectual property widely available for lower prices, because they will now be able to charge, say, a dollar a hit, instead of $10 for a printed copy, to make the same profit on a given work. Yet the white paper contains no promises that consumers will be charged lower prices in exchange for giving up fair use, first sale, and other rights.

History teaches us to be skeptical about claims that giving publishers broad monopoly rights will be in the public interest. During the first centuries after the invention of the

printing press, publishers had considerably stronger monopolies than modern copyright laws grant them. They used these broader rights to charge excessive prices and censor dissenting views. When the English Parliament passed the first modern copyright law, in 1710, it did so in part to stop publishers from oppressing authors, potential competitors, and the public. If the government confers stronger monopolies on publishers again, why should we believe that ubiquitous access and low prices will necessarily result?

Enlarging publisher rights would also provide massive subsidies to the dinosaurs of the Second Wave - today's largely print-based copyright industry, which are terrified of the digital domain and generally don't have the faintest idea about how to market the content in their portfolios on the Net. The only way the entrenched copyright industry can imagine marketing content electronically is through extensive technological locks that will make digital information less free than print information. The white paper gives no thought at all to the needs or concerns of emerging electronic information industries, such as firms that add value to existing information resources, and it seeks to hobble the only kind of Third Wave information service it recognizes - online service providers - by forcing them to undertake the costs of policing users on behalf of the established copyright industry.

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.

It is, in fact, too early in the development of markets for delivery of electronic information products and services to start the kind of heavy-handed government regulation that the white paper would bring about. It would be more sensible to wait to see what kinds of markets emerge and then figure out what, if any, legal fences are needed to avert market failures. Pushing through legislation mandating the maximalist vision before there is public consensus in support of it could backfire by eroding the public's faith in the essential fairness of copyright law.

But the copyright maximalists and their lobbyists are not thinking about how to promote real public respect for copyright law or about what's in the public interest. Their strategy is to rush the white paper's legislation through Congress today and force it down the public's throat tomorrow. You are the public whose throat this policy is about to be forced down. If you don't want it to happen, you'd better do something, and quickly.

How to Get Involved in the White Paper Debate:

The white paper can be found online at http://iitf.doc.gov/.

Opponents of the white paper's recommendations have formed an umbrella group called Digital Future Coalition. Interested parties can post at http://www.dfc.org/dfc.

Bruce Lehman, President Clinton's point man on the proposed legislation, can be reached at:

Assistant Secretary of Commerce and Commissioner of Patents and Trademarks
US Patent and Trademark Office
CPK 2, 2121 Crystal Drive, Arlington, VA 22202
phone +1 (703) 305 8600
PR office phone +1 (703) 305 8341
fax +1 (703) 308 5258
e-mail blehman@uspto.gov

Or contact an administration official with oversight responsibilities for the white paper:

Sally Katzen, Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget
Chair, IITF Information Policy Committee
Old Executive Office Building, Room 350
Washington, DC 20503
phone +1 (202) 395 4852, fax +1 (202) 395 3047
e-mail ipc@a1.eop.gov

The bill's sponsors:

Orrin G. Hatch
United States Senate
SR-131 Russell Senate Office Building
Washington, DC 20510-4402
phone +1 (202) 224 5251

Patrick J. Leahy
United States Senate
SR-433 Russell Senate Office Building
Washington, DC 20510-4502
phone +1 (202) 224 4242
e-mail senator_leahy@leahy.senate.gov

Patricia Schroeder
US House of Representatives
2307 Rayburn House Office Building
Washington, DC 20515-0601
phone +1 (202) 225 4431
fax +1 (202) 225 5842

Carlos J. Moorhead
US House of Representatives
2346 Rayburn House Office Building
Washington, DC 20515-0527
phone +1 (202) 225 4176
fax +1 (202) 226 1279

Thanks to Hal Abelson, John Perry Barlow, Robert Glushko, Peter Jaszi, Mitchell Kapor, Jessica Litman, and David Post for their help with this article.

Pamela Samuelson (pam@sims.berkeley.edu) is a Professor at the University of California at Berkeley with a joint appointment in the School of Information Management and Systems and the School of Law. She is also Co-Director of the Berkeley Center for Law and Technology.