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

Research Publication No. 2000-01
2/2000

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

Jonathan Zittrain

JZ[1] – v 4.8 02/23/00 19:52 **DRAFT**

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

I. Introduction

Individuals have long had the desire but little ability to control the dissemination of personal information about their health. Law has been a weak instrument for such control, given the articulate and powerful interests that insist upon maintaining and enhancing access and use of others' personal information, with sensitive medical data proving only a sporadic exception. Technology has so far only made exploitation of personal information easier. The evolving federal framework for the protection of electronic medical records is, at the moment, one in which individuals are third-party beneficiaries of what are likely to be flexibly-interpreted, ponderously-enforced fair information practices created in the shadow of a Congressionally-mandated networking of sensitive medical data. This networking promises to greatly lower the costs of accessing and using medical data for any number of purposes—including ones not central to health care, such as direct marketing. It is ushering in what some call the "Era of

[1] Author info.

Promiscuous Publication."[2] The danger this era portends is that what is gained in efficiency of health care provision may be lost in erosion of privacy. Privacy advocates could learn a new approach to this problem from an unlikely teacher: publishers of intellectual property—specifically the American music industry.

The music industry until recently feared ruin from the unauthorized swapping and rebroadcasting of high-quality audio reproductions among its customers, a phenomenon enabled by increasingly cheap networks, cheap data storage, and cheap processors—again, the Era of Promiscuous Publication. Despite access to a sympathetic Congress and extensive enforcement resources, the music industry has found recourse to law largely unavailing against this tide of technological progress. The industry is now embarking on a different strategy—changing the technology itself. At the core of the technological response lies the idea of "trusted systems": computer databases of the rights and privileges of specific entities vis- àvis information, linked to hardware and software that recognize and enforce those rights. If fully deployed, trusted systems could trump the Era of Promiscuous Publication with what I call an "Era of Trusted Privication": one in which a well-enforced technical rights architecture would enable the distribution of information to a large audience—publication—while simultaneously, and according to rules generated by the controller of the information, not releasing it freely into general circulation—privication.

In my view there is a profound relationship between those who wish to protect intellectual property and those who wish to protect privacy. Their common desire to control the distribution of information, and the music industry's potential

[2] See Note 6, infra.

success at regaining control through the implementation of trusted systems, offer several lessons to privacy advocates seeking to protect the privacy interests increasingly threatened by the advent of the Era of Promiscuous Publication. I will explore these lessons first by mapping out the problem presented to the music industry by the advent of fast, cheap, and perfect copies, along with the music industry's legal and technological strategies for regaining control. Second, I will describe the similar problem faced by privacy advocates in the arena of medical privacy, the legal solutions that have been and might be attempted, and a hypothetical technological solution that demonstrates the enforcement power of the trusted system. Finally, I will look beyond the enforcement potential of the technological solution to demonstrate how thinking in terms of privication architectures might help negotiate the allocation of rights to medical data to account for the interests of individual "producers" of personal data in ways that need not disparage the legitimate interests of the sophisticated institutional players who wish to consume that data.

II. The Music Industry: A Trajectory of Intellectual Property Worries—and Responses to Them—in a Digitally Networked Environment

A. A New Problem: Quick, cheap, perfect copies

John Perry Barlow laid down the gauntlet to those representing intellectual property interests on February 8, 1996 in a "Declaration of the Independence of

> Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.[3]

The information industries did not need Barlow's help to know fear. The initial consumer boom of the World Wide Web in the mid-nineties spurred widespread and grave concern among authors and publishers—and study among commentators—about a loss of intellectual property protection. The Net featured perfect, cheap, anonymous and quick copying of data; these features and their implications were not lost on wary publishers any more than they were on cyberenthusiasts.[4] As one who identified with the former summarized: "[O]n the

[3] John Perry Barlow, *A Declaration of the Independence of Cyberspace* (visited Nov. 27, 1999) <http://www.eff.org/pub/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration>. John Perry Barlow is co-founder of the Electronic Frontier Foundation, a non-profit organization devoted to protecting privacy and free expression on the Internet. *See* Electronic Frontier Foundation, *About EEF* (visited Dec. 5, 1999) <http://www.eff.org/EFFdocs/about_eff.html>.

[4] *See, e.g.,* Robert A. Cinque, *Making Cyberspace Safe For Copyright: The Protection of Electronic Works in a Protocol to the Berne Convention,* FORDHAM INT'L L.J. 1258, 1258–1259 (1995) ("With the click of a mouse or the tap of a key, virtually anyone with a computer and a

Internet, copying can take place without limits, without visibility, and without cost to the copier; a formula that spells disaster for authors to control use of their works."[5]

In an essay portending massive challenges to copyright law from the Net—if only because even merely viewing information online often entails, as a technical matter, making a copy of it—David Post retells the story of three eras of publishing, the latest ushered in by the Internet:

- Era of Monastic Manuscript: Copyright unnecessary to authors or publishers
- Era of Gutenberg Press: Copyright necessary to authors and publishers
- Era of Promiscuous Publication: Copyright enforcement doubtful.[6]

---

telephone can obtain vast quantities of information from almost anywhere on the globe. These conditions pose a formidable challenge to the international protection of intellectual property. Copyrighted works, which include films, novels, musical works and other forms of expression, are especially vulnerable to piracy."); Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466 (1995) ("The prospect of pervasive audience access to and ability to copy and further disseminate works of authorship challenges the traditional roles not only of information providers - be they publishers, motion picture producers or record producers - but of the individuals who create the works."); Dale J. Ream, *Copyrighted Works & Computer Networks: Is Protection Possible?*, 4 KAN. J.L. & PUB. POL'Y 115 (1995) ("Technology seems to be outpacing the law, and a combination of non-statutory solutions may be the best way to correct the strain on copyright law caused by network technology."); Laurent Belsie, *Who Pays for What On Tomorrow's Internet?* THE CHRISTIAN SCIENCE MONITOR, Oct. 25, 1995, at 1 ("It's a thought that strikes terror in the hearts of entrepreneurs: What if their visions of on-line commerce turn out to be a mirage? What if all the information they hope to sell on the so-called Information Highway is free?"); Ralph Blumenthal, *Thieves in the Idea Marketplace*, THE NEW YORK TIMES, Feb. 11, 1995, at A13 ("[T]echnology is fast outracing the law, and the unauthorized copying, manipulation and sale of creative property, at home and abroad, are disrupting licensing structures that date to the founding of the American Republic."); Jube Shriver, Jr., *Digital Double Trouble: From Rap Music to Medial Formulas, Little Seems Safe From Duplication*, LOS ANGELES TIMES, Apr. 11, 1994, at A1 ("Armed with personal computers and digital recorders, entrepreneurs around the globe are using digital technology in more foreboding ways. They are making unauthorized copies of billions of dollars' worth of music, movies, software, pharmaceutical formulas and other so-called intellectual property.") (hereinafter *Digital Double Trouble*).

[5] Marshall Leaffer, *Protecting Authors' Rights In A Digital Age*, 27 U. Tol. L. Rev. 1 (1995),

[6] David Post, *New Wine, Old Bottles: The Evanescent Copy*, AMERICAN LAWYER, May 1995 at 103. This warning of a data free-for-all on the Internet still echoes today. Several recent headline-grabbing (civil and criminal) crackdowns on alleged music pirating illustrate that the fear of illicit copying is alive and kicking in 1999. *See, e.g.,* Warez Chatters *Busted: Piracy*, WIRED NEWS, Nov. 17, 1999, available at (visited Nov. 28, 1999) <http://www.wired.com/news/mp3/0,1285,32616,00.html> ("The Business Software Alliance is pressing charges against 25 people the organization accuses of trafficking pirated software on the Internet."); *RIAA Suing Upstart Startup*, WIRED NEWS, Nov. 15, 1999, available at (visited Nov. 29, 1999) <http://www.wired.com/news/mp3/0,1285,32559,00.html> (describing the Recording Industry Association of America's civil action against a music software company for contributory

Before the widespread embrace of the Internet, the shape given intellectual property law by Congress and the courts had, along with selective enforcement by public and private entities, led to a coarse détente among authors, publishers, and consumers of intellectual property.[7] This status quo countenanced some level of possibly illegal copying in the world; after all, no law is perfectly enforced. The situation was tolerable, and some even suggested that copying, legal or not, aided authors. A little copying on the margin could be a form of "try before you buy," a means of building reputation or "mindshare,"[8] or even an efficient means of price discrimination—selling at least one copy of a work to a group of related consumers who would not individually buy it at full price.[9]

---

copyright infringement); Bill Schackner, *Carnegie Mellon raids students' PC files over MP3s*, THE DALLAS MORNING NEWS, Nov. 11, 1999, at 6F ("Seventy-one students lost their in-room links to the campus network for the rest of the semester after the school conducted a surprise inspection of computer files and found they had publicly posted audio files containing copyrighted music. The school said it had acted to guard against claims from the recording industry, which a couple of years ago launched a campaign to discourage music piracy among students on technology-oriented campuses, including Carnegie Mellon.").

[7] While international treaty provides for some degree of uniformity of copyright law from one nation to the next (*see Intellectual Property Regimes for the Information Age: Policies of the United States, the European Union and the World Intellectual Property Organization*, 3 B.U. J. Sci. & Tech. L. 9 (1997)), some nations remain outside the web of intellectual property treaties, and with others there exist differing judicial interpretations, levels of actual enforcement, and cultural norms of copying. For example, China has recently entered the web of treaties, but enforcement is still doubtful. *See* Assafa Endeshaw, *A Critical Assessment Of The U.S.-China Conflict On Intellectual Property*, 6 Alb. L.J. Sci. & Tech. 295 (1996).

[8] *See, e.g.,* Laurence Zuckerman*, Lotus Gears Up To Get a Slice Of Internet Pie*, THE NEW YORK TIMES, Sept. 16, 1996, at D1 ("Without 'mindshare' -- the attention of thousands of third-party software developers, industry analysts, trade journalists and customers -- even the best technologies can founder."); Steve Lohr, *The old-media dinosaurs seem to be having a rebirth*, THE NEW YORK TIMES, Mar. 10, 1997, at D5 ("[T]he power of Internet technology . . . has not rewritten the rules of competition for consumer media. Perhaps the most valuable commodity on the Internet is attention, or 'mindshare,' and established brands and mainstream promotion are invaluable in delivering it.").

[9] *See* John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, at 84 ("Familiarity is an important asset in the world of information. It may often be true that the best way to raise demand for your product is to give it away. While this has not always worked with shareware, it could be argued that there is a connection between the extent to which commercial software is pirated and the amount which gets sold. Broadly pirated software, such as Lotus 1-2-3 or WordPerfect, becomes a standard and benefits from Law of Increasing Returns based on familiarity. In regard to my own soft product, rock 'n' roll songs, there is no question that the band I write them for, the

The growth of the Net raised the level of copying exponentially, since it made copying so much easier, the possibility of detection, prosecution and punishment so much more remote, and successive generations of copies as perfectly copyable as originals.[10] Further, few cultural barriers stood in the way of consumers taking advantage of the situation; the norm against copying—especially electronic copying—was and is not as strong, say, as the norm against stealing.[11]

Nowhere is this illustrated so vividly as with the popular music industry. Within the past two years consumers have gained access to, and begun to embrace, technologies that allow them to copy music sold on compact discs

---

Grateful Dead, has increased its popularity enormously by giving them away. We have been letting people tape our concerts since the early seventies, but instead of reducing the demand for our product, we are now the largest concert draw in America, a fact that is at least in part attributable to the popularity generated by those tapes"); Yannis Bakos, Erik Brynjolfsson, and Douglas Lichtman, *Shared Information Goods*, 42 J. Law & Econ. 117 (1999); J.F., *The Shareware Alternative -- The 'try before you buy' market is thriving*, INFORMATIONWEEK, August 14, 1995 at 32; Dan Gutman, *Shareware lets you try before you buy*, SUCCESS, Nov 1996, at 64.

[10] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1196 n.8 (1998) ("The digitalization of information makes simple the reproduction and quick transmission of perfect copies through cyberspace. This technological transformation disturbs the truce that has so far existed between information producers and consumers. Not surprisingly, a fierce battle now rages to revise the law of copyright and establish a new truce in this new technological regime").

[11] See Barlow, *supra* note 8 at 84 ("The laws regarding unlicensed reproduction of commercial software are clear and stern...and rarely observed. Software piracy laws are so practically unenforceable and breaking them has become so socially acceptable that only a thin minority appears compelled, either by fear or conscience, to obey them. When I give speeches on this subject, I always ask how many people in the audience can honestly claim to have no unauthorized software on their hard disks. I've never seen more than 10 percent of the hands go up. Whenever there is such profound divergence between law and social practice, it is not society that adapts. Against the swift tide of custom, the software publishers' current practice of hanging a few visible scapegoats is so obviously capricious as to only further diminish respect for the law"); Software Industry Information Association, *Software Publisher's Association Anti-Piracy Education Initiative* (visited November 26, 1999) <http://www.siia.net/piracy/programs/education.htm> (working to "teach members of the educational community about the responsible and legal use of software"); Hilary Rosen, 1999 WL 988372, ("We also believe in education – letting music fans know that piracy hurts the artists they

perfectly.[12] The entertainment industry has considered this a mortal threat,[13] one that has become particularly acute with the increasing popularity of "MP3" audio compression, a standard that compresses digital music into a package small enough that users can ship music around the Internet without straining their local bandwidth.[14]

The vernacular of music sharing does some justice to the oft-invoked "piracy" label: thanks to MP3 compression and the software built around it, a single person can obtain a music CD, "rip" its tracks onto her hard drive[15] and then "burn" them onto a new blank CD, email them to friends, or even set up a "SHOUTcast" station, broadcasting music live to anyone on the Internet who cares to listen.[16] Testifying before Congress in late 1997, the general counsel of the Recording Industry Association of America put it quite starkly and with only

---

[12] *CD Piracy Soared in 1998, Music Industry Group Says*, NATIONAL POST (April 8, 1999) ("The Recording Industry Association of America said the number of counterfeit compact discs made illegally in U.S. facilities rose to about 338,500, up 163% from 129,000 in 1997. The number of recordings illegally made on blank discs through Internet downloads and other means, rose to 103,971, from a scant 442 in 1997. The figures reflect products that were confiscated on street corners, in flea markets, retail outlets and via Internet sales, the RIAA said.").

[13] *See* Heather D. Rafter, et al., *Streaming Into the Future: Music and Video on the Internet*, 547 Pat/PLI 605, 609 (1999) ("What is different about the Internet's influence on the music business is that it is potentially toppling an industry that has kept control in the hands of a few record labels and sustained high profit margins for a long period of time. Until the advent of the Internet, those few companies seemed invincible, in part protected by a strong legislative scheme and statutory provisions as well as a solid, tightly-controlled method of distribution. Digital distribution of music, that is, the distribution and downloading of music off the Internet, is threatening to change this well-established system.") While the debate has focused on the music industry, other sectors of the entertainment industry have expressed similar concerns. Jack Valenti, President and Chief Executive Officer, Motion Picture Association of America, *Testimony Before Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, U.S. House of Representatives*, Oct. 28, 1999 ("Copyright piracy on the Internet threatens to cause enormous damage to our industry, and to other intellectual property industries. If we are not successful in combating the Internet piracy threat, we could soon be faced with losses that dwarf the dollar amounts we lose today.").

[14] *See* Barak D. Jolish, *Scuttling the Music Pirate: Protecting Recordings in the Age of the Internet*, 17 SPG Ent. & Sports Law 9 (1999).

[15] See Audiocatalyst (visited Nov. 29, 1999) <www.xingtech.com> for one such program.

[16] See (visited Nov. 29, 1999) <www.shoutcast.com>, where the enabling software is available for free and a list of individuals' "radio" stations is maintained.

slight hyperbole: "Today, one individual, in less time than it takes me to read this testimony, can send a full-length album to more than fifty million Internet users."[17]

The publishing industries initially responded by using their political power to broaden and strengthen the scope and application of legal protections against unauthorized copying of their work. However, as it became clear that the problem would not be overcome by additional difficult-to-enforce legal rules, the music industry has turned to technology backed by law as a more promising avenue for redress. An examination of each of these types of responses, legal and technical, yields possible ways that privacy advocates can ultimately benefit from the lessons of the music industry's experience.

B. Solution 1.0: Buttressing Copyright and Contract

Those who worried about the Net's effect on intellectual property were not idle; as a first step, they called for—and in many cases, got—a strengthening of intellectual property laws and public enforcement to counter the sea change in information-sharing abilities wrought by the Net.[18] Some of these provisions

[17] Testimony of Cary H. Sherman, *Internet Piracy and H.R. 2265, the "No Electronic Theft Act,"* Sep. 11, 1997, 1997 WL 566007 (F.D.C.H.). A variety of portable music players are now on the market; users can put copies of songs in MP3 format onto the players and then listen without being near a personal computer. *See* (visited Nov. 29, 1999) <www.rioport.com>.

[18] *See* Belsie, *Who Pays for What On Tomorrow's Internet, supra* note 15 ("[P]ublishers are pushing a traditional approach, asking that existing copyright laws be strengthened. Last month, this argument got a huge boost from the Clinton administration. Its white paper "Intellectual Property and the National Information Infrastructure" recommended much the same thing."); Mitch Betts, *Pirates lurk on the info highway; Increased concerns cause publishers to pull material off the Internet*, COMPUTERWORLD, Jul. 25, 1994, at 60 (describing a Clinton administration proposal for "fine-tuning the federal copyright laws" to address" digital copying); Jeff Leeds, *Cyberspace Copyright Proposal Draws Praise*, LOS ANGELES TIMES, July 8, 1994, at D1 ("Endorsing a first, tentative step toward modernizing the nation's intellectual property laws, the entertainment and information industries today welcomed a draft recommendation from the Clinton Administration on extending copyright law to cover on-line services and other corners of

were specifically designed to increase penalties for copying using electronic means.[19] The music industry in particular sought to protect itself by making extensive use of the private right of action for federal copyright violations.[20] The existence of this right presumably helps to prevent at least some forms of open, static and notorious music piracy from taking place through the World Wide Web. Even in a crowded domain name space,[21] no one has dared to reserve, much less place content within, say, <www.piratedmusic.com> or <www.stolensingles.com>.[22] At least one music industry group is working hard on new technologies that can identify threads of streamed music coursing

---

cyberspace."); Michael D. McCoy and Needham J. Boddie, II, *Cybertheft: Will Copyright Law Prevent Digital Tyranny on the Superhighway?*, 30 WAKE FOREST L. REV. 169 (1995) ("Given the vital importance of an integrated superhighway, government likely will take certain regulatory steps to garner industry support. Revising the current copyright laws may provide the necessary protection to prevent technological isolation."); Shiver, *Digital Double Trouble*, *supra* note 17 (describing efforts by the Recording Industry Association of America to strengthen and reform copyright law in the digital context); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999) (discussing the trend towards criminalization of intellectual property infringement in reaction to the increased ease of transferring information by computer and the Internet); *You can run, but you can't hide; industry revs up new campaign to bag corporate software pirates*, COMPUTER SHOPPER, August 1991, at 107; Paul M. Eng, Ed., *Keelhauling Software Pirates*, BUSINESS WEEK, February 18, 1991 (reporting the Software Publisher's Association cracking down on corporate software piracy).

[19] *See* No Electronic Theft (NET) Act. Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amendments to 17 U.S.C. 101-803, and 18 U.S.C. 2319) (Specifically, NET makes it a felony to violate 17 U.S.C. §506(a)(2), under penalty of imprisonment or fines under 18 U.S.C. §2319(c)); Stephanie Brown, *The No Electronic Theft Act: Stop Internet Piracy!* 9 DePaul-LCA J. Art & Ent. L. 147 (Fall, 1998).

[20] 17 U.S.C. 502-505; *see Recording Industry Reinforces Its Strategy to Fight Against Internet Piracy*, EUROPEAN REPORT, Nov. 4, 1999 ("The International Federation of the Phonographic Industry (IFPI) has unveiled a new coordinated global strategy against Internet piracy, announcing actions against hundreds of infringing sites in more than 20 countries world-wide. This strategy was put in place by allied national groups of the IFPI in the form of warning letters and legal initiatives."); *Hunting Pirates*, PC MAGAZINE, Dec. 14, 1999 at 11 ("The music industry is taking aim at allegedly illegal music files posted on the Internet. In a global antipiracy effort, the International Federation of the Phonographic Industry (IFPI) says that it is implementing legal actions designed to shut down sites offering illegal music files."); Courtney Macavinta, "Teen Charged In Connection With DVD Cracking Tool, CNet News.com <http://news.cnet.com/news/0-1005-200-1531192.html?tag=st.ne.1002>.

[21] *See* Matt Richtel, *New Domain Names Set a Record in 1998*, N.Y. TIMES, Jan. 28, 1999, at G3.

[22] See Network Solutions, Inc., *Whois Queries*, (visited Nov. 29, 1999) <http://www.networksolutions.com/cgi-bin/whois/whois/> (no match for "piratedmusic.com" or

through the data flows of the Internet-at-large, for the purposes of hunting down and suing (or at least threatening) music pirates.[23] Additionally, the Digital Millennium Copyright Act's[24] provision for expedited subpoenas to Internet service providers seeking the identities of people posting unauthorized copyrighted material has been well-used.[25]

A litigation win is not always necessary to achieve an important industry goal: the Recording Industry Association of America recently lost its lawsuit challenging the production of the "Rio" portable MP3 music player under the Audio Home Recording Act,[26] but the manufacturers of the Rio are now cooperating with the RIAA towards the creation of a "secure" music format.[27]

Second, to provide for protection in areas where copyright law is ambiguous or silent, or simply to buttress the default rights copyright provides, publishers have increasingly used mass contracting to enhance control over that which they

---

[23] *See* Alice Rawsthorn, *Industry Plans New Round of Tests to Build Defences Against Internet Piracy*, FINANCIAL TIMES, Jun. 4, 1998, at 8. ("The adoption of an industry-wide system to identify digital musical signals is regarded as one of the most important technical safeguards. Such a system would use embedded signalling technology to enable companies to monitor any broadcasts of their music, and whether any royalties are owed to them."); Barak D. Jolish, *Scuttling the Music Pirate: Protecting Recordings in the Age of the Internet*, 17 SPG Ent. & Sports Law. 9, 10 (1999) ("The RIAA … employs three full-time staffers and a variety of technological aids to uncover illegally posted music. Using hundreds of warning latters and a handful of lawsuits, in 1997 the RIAA alone shut down more than 250 sites, many originating from [account holders at] universit[ies].").

[24] *See* notes 92 and 94, infra and accompanying text (discussing the DMCA).

[25] *See* Jack Valenti, *Access to Digital Entertainment on the Internet*, Testimony, Oct. 28, 1999, 1999 WL 988371 (F.D.C.H.).

[26] Recording Indus. Ass'n Of America v. Diamond Multimedia Sys.,180 F.3d 1072 (9th Cir. 1999);

[27] *See* Testimony of Rondal J. Moore before the House Commerce Committee Subcommittee on Telecommunications, Trade and Consumer Protection, *WIPO One Year Later: Assessing Consumer Access To Digital Entertainment On The Internet And Other Media*, Oct. 28, 1999 ("While we were gratified that the U.S. Court of Appeals for the Ninth Circuit ruled in our favor, we take greater satisfaction in the subsequent cooperation between the recording, computer, Internet and consumer electronics industries to craft interoperability standards for copy protection systems under the rubric of the Secure Digital Music Initiative."); *House Hearing Reopens Digital Copying Debate*, 11 AUDIO WEEK 43, Nov. 1, 1999 (quoting RIAA president Hilary Rosen as saying she was almost glad to have lost the lawsuit that allowed MP3 players into the market).

wish to share only so far.[28] The leading case in this area remains *ProCD v. Zeidenberg,* in which a company that placed telephone directory "white pages" data on a CD-ROM for consumer use was able to prevent a purchaser from allowing the public at large to access his single copy of the CD-ROM over the Internet for a fee.[29] Copyright law might well not have protected ProCD's data, [30] but the "shrinkwrap" license—the wording on and inside the box stating the terms by which a purchaser such as Zeidenberg could use the software should he choose to keep it—achieved a restriction on redistribution in copyright's probable absence.[31] The "extra" rights provided for by contract were found not to run afoul of federal copyright preemption doctrine because they were generated through voluntary agreement between the parties.[32] Whatever the wisdom of *ProCD's* holding—and much has been written on the subject—it is part of a larger trend by which restrictions on information through public right are strengthened by the application and enforcement of contract doctrine.[33] Indeed, efforts to have the American Law Institute adopt a new section 2B of the Uniform Commercial Code were expressly designed to make it clearer under state law that simply clicking upon "I agree" while online might be enough to form a contract—one with quite

[28] *See* Katie Hafner, *It May Be Boilerplate, But Read Before You Click*, N.Y. TIMES, Apr. 16, 1998, at G3; David Nimmer, Elliot Brown, and Gary N. Frischling, *The Metamorphosis of Contract into Expand*, 87 Calif. L. Rev. 17 (1999) ("publishers who follow the logic of ProCD, Inc. v. Zeidenberg may amplify their statutory rights simply by wrapping books in cellophane").
[29] 86 F.3d 1447 (7th Cir. 1996).
[30] *See* note 19, supra.
[31] ProCD, 86 F.3d at 1449.
[32] 17 U.S.C. § 301 (1999) (Federal copyright preemption); ProCD, 86 F.3d at 1453-55.
[33] *See generally* Brian Covotta & Pamela Sergeeff, *Contract Enforceability: ProCD, Inc. v. Zeidenberg*, 13 Berkeley Tech. L.J. 35 (1998); Dennis S. Karjala, *Copyright Owners' Rights And Users' Privileges On The Internet: Federal Preemption Of Shrinkwrap And On-Line Licenses*, 22 Dayton L. Rev. 511 (1997).

powerful, even surprising terms.[34] While the adoption of U.C.C. 2B has stalled, a sibling effort is underway through UCITA.[35]

Enhanced mass contracting is not yet a particularly important or powerful weapon for the music industry in its current battle against music piracy. After all, unlike the telephone directory information in *ProCD,* original music is already clearly and thoroughly (at least in theory) protected by copyright, so there are fewer gaps in control for contract to fill.

Although these two strategies have no doubt helped to minimize large-scale, centralized domestic music piracy, the practical difficulties of enforcing the legal regime in the face of millions of individuals downloading and sharing MP3 files has driven the music industry to turn to technology for an effective way to regain and even sharpen its earlier control. As one scholar put the problem of intellectual property on the Internet: "This is the law's version of the Laffer Curve: Just as tax revenues supposedly increase and then drop off as tax rates rise, so too, as copying becomes easier and easier, laws to protect an author's right to prevent unauthorized copying become more and more valuable—until, perhaps,

---

[34] *See* U.C.C. Art. 2B (Draft, Aug. 1, 1998) (visited Nov. 26, 1999) <http://www.law.uh.edu/ucc2b/080198/080198.html> (reporter's official draft of proposed revisions to Uniform Commercial Code Article 2B); Mark Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. Cal. L. Rev. 1239 (1995); Lawrence Lessig, *Sign It and Weep*, INDUSTRY STANDARD, Nov. 20, 1998; A. Michael Froomkin, *Article 2B as Legal Software for Electronic Contracting - Operating System or Trojan Horse?*, 13 Berkeley Tech. L.J. 1023 (1998); Maureen A. O'Rourke, *Progressing Towards a Uniform Commercial Code for Electronic Commerce or Racing Towards Nonuniformity?*, 14 Berkeley Tech. L.J. 635 (1999); Jane C. Ginsburg, *Authors as "Licensors" of "Informational Rights" Under U.C.C. Article 2B*, 13 Berkeley Tech. L.J. 945 (1998); David A. Rice, *Digital Information as Property and Product: U.C.C. Article 2B*, 22 U. Dayton L. Rev. 621 (1997).

[35] *See Uniform Computer Information Transactions Act, Draft for Approval* (visited Nov. 26, 1999) <http://www.law.upenn.edu/bll/ulc/ucita/citam99.htm>; Robert Fox, *UCITA Latest*, COMMUNICATIONS OF THE ACM, Sept. 1999 at 9; UETA (uniform electronic transactions act) and H.R.1714 (Electronic Signatures in Global and National Commerce Act) and S. 761 (Third Millennium Electronic Commerce Act).

a point is reached at which copying has become so simple, so costless, that regulation becomes virtually impossible."[36]

C. Solution 2.0: Technological self-help through trusted systems

Within the past five years, a new strategy has come to the fore to deal with the impact upon information sharing (or, from the point of view of those who wish control, "piracy") by cheap processors, networks, and storage—a strategy quite different from the incrementalism of tighter enforcement of substantively stricter rights, whether through public law or private contract. The strategy is ambitious, with a fantastic payoff of control to publishers generally, and the music industry specifically, if it can be accomplished.

The premise is simple: the Net of today is what we have made it—and the Net of tomorrow will be however we *re*make it.[37] Each need not bear much resemblance to the other. Publishing executives who think that the unfortunate ease of information flow is an inherent quality of the Internet—indeed, a necessarily ever-accelerating one—suffer from "is-ism."[38] So do neo-libertarians who think that the Net's current unsuitability to regulation is simply a fact of life to be celebrated rather than an architectural decision that once made may still require sustained practical if not theoretical defense. The clich éthat the Internet

[36] *See* David Post, *New Wine, Old Bottles* at 103
[37] *See* Lawrence Lessig, Code and Other Laws of Cyberspace, (New York: Basic Books, 1999).
[38] *Id* at p. 24 (Lessig defines is-ism as confusing how something is with how it must be.)

"recognizes censorship [and presumably information blockage from any source] as damage and routes around it" has perhaps prematurely achieved the stature of truism.[39]

How could a future Internet realistically tame the current information chaos? Mark Stefik, a researcher at Xerox PARC, has been quietly developing and touting an answer for several years. Stefik is among the leading architects of so-called "trusted systems," technological gatekeepers that allow "authorized" flows of information while flatly blocking "unauthorized" uses.[40] A necessary element is the ability to structure "rights" into a calculable framework that is then automatically enforced by the technology, whether the user pleases or not. To the extent that these rights architectures are made secure—when, through a combination of hardware and software, a user who is anything less than a talented hacker is truly constrained by the system at the behest of whoever is the source of the information it might display—the system can be said to have "trust." A trusted system is one that can be trusted by a rights-holder as against the user of the system—even if the physical system is in the custody of the user. (This use of the word "trust" is a term of art that should not be confused with its colloquial meaning, a point I explore in Section III.)

---

[39] *See* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. Cinn. L. Rev. 177, 178 n.3 (1997) (crediting John Gilmore with the phrase and discussing its apocryphy).

[40] Mark Stefik, The Internet Edge, (MIT Press, 1999), 197-231 (comparing the effect of technology on copyright and privacy, describing the threat to privacy on the Internet and describing privacy, secrecy and anonymity preserving technologies). Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 Berkeley Tech. L. J. 137 (1997). Mark Stefik, *Trusted Systems*, SCIENTIFIC AMERICAN, Mar. 1997, at 78.

Multi-user operating systems have long had rudimentary "rights" architectures.[41] Files have "owners." Owners can specify who else on the system can view the file. They can independently specify who else on the system can alter the file—indeed, some might be permitted to view the file without altering it, while others might be permitted to alter the file without viewing it. Owners can even alienate the right to assign new rights: a simple command transfers ownership to another user. In more sophisticated systems, "audit trails" reveal to the owner (or to proxies to whom the owner has delegated the relevant right) who among those authorized has peeked at a file and when.

Thus, a trusted system might include a vernacular through which a publisher could tag a document as "not to be copied, in whole or in part." A consumer could be sent the document—put more precisely, might have "read access" to it—but upon attempting to highlight a portion, copy it, and paste it elsewhere—perhaps in an email to send to a friend—would receive an admonition from the computer that says "operation not allowed." Or a publisher might label the document with a fifty-cent printing fee, and upon asking for a printout the consumer would, in turn, be asked by her computer to pay fifty cents. No payment, no printout.[42]

---

[41] The Official Red Hat Linux Getting Started Guide, *Ownership and Permissions* (visited Nov. 29, 1999) <http://www.redhat.com/corp/support/manuals/RHL-6.0-Manual/getting-started-guide/gsg/doc026.html> (a sample of text from a UNIX manual using rights language); Erik's Linux Page, *Dealing with User rights* (visited Nov. 29, 1999) <http://www.lysator.liu.se/~forsberg/linux/about-chmod.html>; Microsoft Technet, *User rights control by User*, <http://technet.microsoft.com/cdonline/default-f.asp?target=http://technet.microsoft.com/cdonline/content/complete/windows/winnt/winntas/manuals/concept/xcp01.htm>.

[42] For a description of at least one kind of trusted system with an eye towards intellectual property protection, *see* Mark Gimbel, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law*, 50 Stan. L. Rev. 1671 (1998).

Further, tying nuanced forms of access to information to one's identity or characteristics enables highly targeted price discrimination. One could give access to a text at "retail" price to a businessperson and at a discount to a student; one could let certified Democrats see something that Republicans (or at least non-Democrats) could not.[43]

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

Songs are not "sold" in even the colloquial sense of the word; rather, they are "licensed"—both from a legal and technical standpoint. Compact discs have joined 8-tracks, cassettes, and phonograph records in the dustbin; their replacements are small, generic "jukeboxes" linked by the Net to a central repository of songs managed by a publisher.[44]

An individual authenticates herself to a jukebox—perhaps with a fingerprint or carefully scrawled signature on its back with a stylus—and then may access specific songs that fall under her monthly payment plan. She will be granted access to the music archive only after parting with personal information about herself, including name, age, address, and phone number. (This information is passed in a heartbeat to the publisher from her personal computer's registration

[43] Judge Easterbrook saw the value of price discrimination as a reason to uphold the contract in *ProCD,* where the consumer version of the software in question cost less than one intended for commercial use. Zeidenberg owned the cheaper consumer version, the license of which duly limited his use of the software. *See* Kalama M. Lui-Kwan, *Digital signatures: Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 Berkeley Tech. L.J. 463 (1999); ProCD at 1450.

[44] See Paul Goldstein, "Celestial Jukeboxes", chapter 1.

module; she entered and authenticated it once, and it is now requested constantly as she uses the computer to visit various web sites. She has long since set her "preferences" to release it if access to the site will be denied otherwise.[45])

As she selects songs, her tastes are noted, allowing offers for "special" songs not included in her monthly plan to be specifically targeted to her tastes and sent to her across all media.[46] The songs she asks for are "streamed" to her player as she listens, and do not remain there any more than a song stays inside a radio after it is over.

An inaudible signal is embedded in the music; if she holds a microphone to her headphones and thereby makes an imperfect, analog copy to an old-fashioned cassette, her name and a unique identifier will be "in" it, permitting prosecution for copyright infringement if the copy is found.[47] Her user license agreement provides an alternative path for the music owner to pursue fast-track damages, including the sending of a signal to her jukebox that permanently disables anyone from using it until the matter is settled.

In the unlikely event that she were to abuse her access to the system by hooking up her jukebox to an amplifier and playing the music at a backyard party

---

[45] *See* note 197, infra, for a description of "P3P," the beginnings of such a "privacy enhancing" system.

[46] *See,* Hilary Rosen, President and Chief Executive Officer, Recording Industry Association of America, *Testimony Before Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, U.S. House of Representatives*, Oct. 28, 1999 (describing and extolling a similar customized marketing approach and noting that "many sites already make customized music recommendations to returning clients based on their buying history")

[47] Kenneth Dam, *Self-Help in the Digital Jungle*, 28 J. Legal Stud. 393 (1999); Geoff Nairn, *Yet to Make its Mark: Technolgy Digital Watermarks*, LONDON FINANCIAL TIMES, March 15, 1999, at 12; Air Force Research Laboratory, *Digital Watermarking Technology* (visited Nov. 29, 1999)

outside her California apartment, a cheap listening post on the beach's lifeguard chair could be monitored by ASCAP,[48] which would use a watermark decoder to know instantly that she was behind the cacophony—and that the particular performance had only been paid for at the "portable personal use" rate rather than the "noncommercial party" rate. (Music data from listening posts might be shared with ASCAP by the local police department, which has deployed a network of microphones around the city to respond to the sound of gunshots in the area.[49])

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

A world like this is still at least five years off by my conservative reckoning—and the music industry may, after consulting its own muses and the market, elect not to invoke all the technical power that could be at its disposal. Still, publishing industries have already taken the first halting steps towards trusted systems architectures.[50]

<http://www.rl.af.mil/div/IFB/techtrans/datasheets/H2Omark.html> (describing watermarking technology and its uses, military and otherwise).

[48] *See* note 47 supra.

[49] *See* Greg Miller, *Big Ear of the Law Tames Town's Gunfire; Crime: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunshots*, LOS ANGELES TIMES, Jan. 12, 1998 at D3; *see also* ShotSpotter home page (visited Nov. 29, 1999) <www.shotspotter.com> (commercial vendor of distributed listening products).

[50] Adobe Systems has designed a popular document system that enables the distribution of "read only" written work. "Read only" refers to a document that may be viewed but not edited by the reader. *See* Adobe, *Products: Acrobat* (visited Nov. 27, 1999) <http://www.adobe.com/products/acrobat/main.html>. An online bookseller

complements an array of traditional books and magazines with "e-matter," downloadable over the Internet for a fee—and readable only on the physical computer to which it is registered. *See* Fatbrain.com, *What is e-matter* (visited Nov. 27, 1999) <http://www.fatbrain.com/ematter/e_whatis.html>. One legal scholar has just released a novel as e-matter. *See* James Boyle, The Shakespeare Chronicles on Fatbrain.com (visited Nov. 27 1999) <http://www1.fatbrain.com/asp/bookinfo/bookinfo.asp?theisbn=EB00003261>. DIVX technology was a short-lived standard for mass-producing and distributing audio-visual content that a user could watch or listen to only a limited number of times. Its roots go back to the technology fictionalized in the television series "Mission: Impossible"; each episode began with a reel-to-reel tape that self-destructed after playing a message intended only for one person's ears. DIVX was recently abandoned as a digital video standard, unable to compete with the more popular DVD format. *See* Peter Spiegel, *Format war*, FORBES, May 17, 1999 ("Circuit City's…big mess is its Digital Video Express (Divx) system -- specially encrypted $4.49 videodisks that can be viewed as many times as you want in a 48-hour period; and they don't have to be returned. DVD…is a $20 disk you can keep and play as many times as you want"); Maryanne Murray Buechner, *Just as DVD is declared a winner in the consumer market, a new entry called Divx tries to change the rules*, TIME DIGITAL, April 12, 1999 ("Divx (rhymes with civics, short for Digital Video Express) is a feature on selected DVD players that--paradoxically--allows you to rent movies you'll never need to return. Divx discs are encrypted dvds that can be decoded and played only on a machine that has the Divx chip; the deck also has a modem that uses your home's regular phone line to communicate with a sort of "Divx Central." The player dials in the first time you want to use it, then again once a month to take care of the billing"); *Digital Video Disarray*, The Washington Post, June 25, 1999 at N70. Manufacturers of DVD players have experimented with "regional DVD" formats, whereby individual players can be associated with various regions of the world. Individual disks of audiovisual material could be coded only for one region, enabling a more trusted temporal staggering of film and video releases across international boundaries for price discrimination purposes. *See Matshushita Plans Regional DVD Formats*, OPTICAL MEMORY NEWS, Jun. 18, 1996. In the United States, digital audio tape players are designed to refuse to copy a copy. The Audio Home Recording Act, 17 USC § 1002 reads in relevant part:

> (a) . . . No person shall import, manufacture, or distribute any digital audio recording device or digital audio interface device that does not conform to--
> (1) the Serial Copy Management System;
> (2) a system that has the same functional characteristics as the Serial Copy Management System and requires that copyright and generation status information be accurately sent, received, and acted upon between devices using the system's method of serial copying regulation and devices using the Serial Copy Management System; or
> (3) any other system certified by the Secretary of Commerce as prohibiting unauthorized serial copying.

It is worth noting that the he AHRA itself provides no definition for "Serial Copy Management Nimmer notes, "the result is that the enacted text, standing alone, cannot be interpreted; resort to legislative history of the bill -- in particular, to the Technical Reference Document that contained the specifications for the SCMS -- is therefore unavoidable." NIMMER

For the music industry, these steps entail the development of a standard in cooperation with hardware and software developers called the Secure Digital Music Initiative, or SDMI, to replace MP3. Its protocols—still in flux—contemplate many of the features hypothesized above.[51]

To be sure, these steps are merely beginnings, and they include as many failures as successes.[52] However, there are reasons why the music industry appears to be placing its faith in technology, knowing full well that the industry's interests cannot be assumed to be identical to those of the hardware and software vendors who would have to support trusted technology, and that a

---

ON COPYRIGHT, Ch. 8b. The Audio Home Recording Act of 1992, § 8B.03. Despite the technical abstruseness of these specifications, Nimmer states with some certainty a simple principle of serial copying under the act: "The controls of the SCMS . . . prevent making copies from all but original recordings. Accordingly, a first generation copy may be played on a tape deck/recorder equipped with an SCMS and enjoyed in one's living room; it may not, by contrast, be used to make additional copies."

[51] According to the Recording Industry Association of America's website, SDMI "will answer consumer demand for convenient accessibility to quality digital music, enable copyright protection for artists' work, and enable technology and music companies to build business models for consumers that will expand the availability of music on-line." Recording Industry Association of America, *Technology*, (visited Nov. 19, 1999) <http://www.riaa.com/tech/tech_sd.htm>; *See also*, Jennifer Sullivan, *RIAA Unveils Anti-MP3 Plan*, Dec. 15, 1998, (visited Nov. 29, 1999) <http://www.wired.com/news/news/culture/story/16853.html> ("SDMI poses a challenge to MP3, a prolific but controversial audio format that compresses music files at near-CD-quality sound for easy distribution over the Internet. Users love its convenience, but the RIAA says the technology allows for massive music piracy. The RIAA is calling for more security in the new format.").

[52] The protections by which the first generation of DVDs was to be uncopyable were cracked recently. See Mike Musgrove, *Hackers Unlock Hollywood DVD Code; Encryption Mistake Allows Film Copies*, THE WASHINGTON POST, November 4, 1999 ("The system used to protect DVD-formatted movies from being copied--a feature that took years for the entertainment industry to agree on before it would green-light this popular technology--has been cracked. A group of programmers has duplicated the software equivalent of a skeleton key and placed it on the Internet for anyone to download. Using this tiny program, anyone owning a personal computer with a DVD-ROM drive--an increasingly common feature--can unlock a DVD movie and record a perfect digital copy of it onto his hard drive"); Josh Chetwynd, *DVD 'key' changed after copy protection cracked*, USA TODAY, November 9, 1999 at 3D ("The news did not stun Motion Picture Association of America (MPAA) chief Jack Valenti, who recently testified that it was "only a matter of time" before the technology, once considered unbreakable, was compromised. But the revelation has left DVD manufacturers scrambling to protect the burgeoning business from being hurt by the prospect of future piracy.") (New DVDs are encoded using a different, uncracked method.)

number of independent creative minds will be bent on breaking any locks it might convince the institutional technologists to come up with.

At least one formal process has at last coalesced through which a new generation of computer hardware can augment the software of "trust," demonstrating cooperation between content providers and consumer systems architects, and posing a new kind of challenge to those who would seek to crack the code. The Trusted Computing Platform Alliance was formed to little fanfare in October 1999, by the most powerful companies in information technology:[53]

> The Trusted Computing Platform Alliance, or TCPA, was formed by Compaq, HP, IBM, Intel and Microsoft. All five companies have been individually working on improving the trust available within the PC for years. These companies came to an important conclusion: the level, or "amount", of trust they were able to deliver to their customers, and upon which a great deal of the information revolution depended, needed to be increased and security solutions for PC's needed to be easy to deploy, use and manage. An open alliance was formed to work on creating a new computing platform for the next century that will provide for improved trust in the PC platform.[54]

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

The ambition of this technical strategy in response to the panic over the Internet free-for-all is to hasten a new era (or perhaps take us back to an earlier

---

[53] See Trusted Computing Platform Alliance, *Compaq, HP, IBM, Intel, and Microsoft Announce Open Alliance to Build Trust and Security into PC's for e-Business*, (visited Nov. 27, 1999) <http://www.trustedpc.org/press/pdf/TCPA%20Press%20Rel.7.pdf.>

[54] Trusted Computing Platform Alliance, *Home Page* (visited Nov. 27, 1999) <http://www.trustedpc.org/home/home.htm>.

one) before the current one has truly settled in. We might revise Post's recounted timetable as follows:

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

The term "privication" is meant to capture the heretofore-unlikely coupling of mass distribution of information to "authorized" users with tight control over its use—at least along the dimensions of perfect, instantaneous, and anonymous copying.[55] That control is enabled through private rather than public means, eliminating the need for copyright to the extent that the trusted system can be relied upon to protect information.[56]

There is a caveat to this use of private means: the government has been asked by publishers to buttress the security of an imperfect privately deployed trusted system by penalizing those who crack it. The Digital Millennium Copyright Act does just this, providing for civil and criminal penalties for those who circumvent technological protection measures, and in some cases for those who simply make available technologies that can be used for circumvention (and little else).[57] Passage of the DMCA was a high priority for the entertainment

[55] The first and only time I have heard the term used was at a 1998 Harvard/MIT conference in which invited scholars commented on student work. See "The Legal/Technical Architecture of Cyberspace" Dec. 6, 1998, at Berkman Center For Internet and Society, *conference description*, (visited Nov. 27, 1999) <http://cyber.law.harvard.edu/architect.html>.

[56] Pamela Samuelson noted this possibility as early as 1994. *See* Pamela Samuelson, *Will the Copyright Office be Obsolete in the Twenty-First Century?*, 13 Cardozo Arts & Ent. L.J. 55, 58-60 (1994) ("Why would one need copyright protection, let alone need to register a claim of copyright with a Copyright Office, if it becomes virtually impossible to copy a work because of the technological protection attached to it?").

[57] See 17 U.S.C. 1201. The prohibitions are stayed while the Library of Congress analyzes what exceptions—such as fair use—should exist to permit users to attempt to crack an otherwise-covered system. Note that these exceptions would still only be defensive privilege against prosecution by someone who had successfully cracked a trusted scheme. They do not grant an easement-like right of access, only a right to attempt to break in, with the owner entitled to lock

industry, and by all accounts its power in the development of the legislation was as strong as with other copyright-related matters taken up by Congress—and the power of disparate "fair use" interests correspondingly weak.[58]

The DMCA's proscriptions are worded in a way that may protect only those trusted systems that contain copyrighted works in the first instance: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[59] Works protected under Title 17 are works protected by copyright. But this limitation could become a lively area of interpretation. If a trusted system is deployed to protect both copyrighted and non-copyrightable material—whether in the same physical database or not—would cracking the database to gain access solely to the noncopyrightable material be punishable under the DMCA? If so, it is possible that trusted systems covering large databases of unprotectable information[60] could be brought under the DMCA's protection by the mere presence of a copyrighted work elsewhere in the database. However this issue is resolved—and I do not mean to suggest that it will be particularly more vexing than the statutory interpretation issues that courts face every day—it shows that government can

---

the property up as tightly as possible. *Cf.* Brown, *Copyduty*, *supra* note 99, at ¶¶ 8 - 9 (comparing fair use under a hypothetical "copyduty" regime to a public easement in real property). For a critique of the DMCA's scope, *see* Pamela Samuelson, *Why the Anti-Circumvention Regulations Need to Be Revised*, 14 Berkeley Tech. L.J. 519 (1999).

[58] *See* Malla Pollack, *The Right To Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause and the First Amendment*, 17 Cardozo Arts & Ent. L.J. 47 (1999) (describing the Digital Millenium Copyright Act as "butchering fair use"); Andrew L. Shapiro, *The Disappearance Of Cyberspace And The Rise Of Code*, 8 Seton Hall Const. L.J. 703, 719 n.44 (1998) ("It is safe to assume, by this presumption of virtual displacement, that many materials previously distributed physically (books, CD's, etc.) with a traditional intellectual property balance between fair use and exclusive control will likely be disseminated online with trusted systems and no such balance.")

[59] *See* 17 U.S.C. 1201.

[60] *See* Feist, 499 U.S. 340.

choose to enhance the effectiveness of private information control regimes, even aside from legislating substantive information property rights or enforcing contracts.[61]

Indeed, the music industry appears to credit the DMCA for adding steam to the early stages of its Secure Digital Music Initiative—not just for protecting the final result, but for implicitly urging technology companies to take the music industry's call for a trusted system seriously.[62] The story of effective privication so far requires the manufacturers of hardware and software to design new technologies with publishers, rather than consumers, as the "customers" to whom they respond. In the case of the Trusted PC Alliance, the members appear to comprise only the manufacturers.[63] There exist advisors, but their identities are not currently available to non-members.[64]

The music industry—in a split with the motion picture industry—has recently tempered its cries of falling skies,[65] and a recent spate of cooperation with technologists over SDMI may be why. Relations with the company producing portable MP3 players have been patched,[66] and the president of the RIAA now says that the "rocky marriage" of the technology industry and the creative

---

[61] *See* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. Cinn. L. Rev. 177, 201 (1997) ("The Internet Trinity tells us that information wants to be free and that the thick fingers of Leviathan are too clumsy to hold it back. The position is less clear if that information is guarded by digital fences which themselves are backed by a state power maintained through private systems of surveillance and control.")

[62] *See* Rosen, *Testimony Before Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, U.S. House of Representatives*, Oct. 28, 1999, *supra* note 83 ("Enactment of the DMCA ended years of antagonism between the entertainment and copyright industries and the technology and consumer electronic industries.")

[63] *See* TCPA, *List of Members* (visited Nov. 27, 1999) <http://www.trustedpc.org/home/members.htm>.

[64] *See* TCPA, *List of Advisors* (visited Nov. 27, 1999) <http://www.trustedpc.org/home/advisor.htm>, which requires a password for access.

[65] *See House Hearing Reopens Digital Copying Debate*, 11 AUDIO WEEK 43, Nov. 1, 1999.

community is now on much firmer ground.[67] The SDMI boasts more than 110 companies in the music, consumer electronics, and technology industries, enjoying a "mutuality of interests" flowing from Congress's DMCA framework.[68] Consumers do not have a seat at the table, only an ultimate veto in the marketplace.[69]

An agreement among the members of the alliance on trusted systems standards could potentially limit the choice of information technology environments among consumers—whether these consumers are publishers or readers of information. The courts might thus theoretically intervene for antitrust reasons and then assert general policy interests as well, though they have been loathe to do so in other private standards-settings efforts, perhaps because agreement to achieve interoperability can be so beneficial.[70] And, as we have seen, Congress has been clear about its willingness to foster such initiatives.

Having Congress merely foster such initiatives, rather than mandate a specific technology solution, may be preferable to both the technology industry

---

[66] See note 27, supra.
[67] *See* Rosen, *Testimony Before Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, U.S. House of Representatives*, Oct. 28, 1999, 1999 WL 988372; *supra* note 79.
[68] *Id*. (rosen testimony)
[69] *See, e.g.,* Michael Robertson, *Playing The SDMI Blues*, MICHAEL'S MINUTES, June 30, 1999, available at MP3.com's web page (visited Nov. 29 1999) <http://bboard.mp3.com/mp3/ubb/Forum8/HTML/000038.html> ("While the RIAA touts the "openness" of the process, it is anything but open to the public.").
[70] *See* Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 Conn. L. Rev. 1041 Summer, 1996 at 1079 ("the Sherman Act should treat joint standard-setting organizations as generally procompetitive forces in standardized markets, and that antitrust scrutiny of such groups should focus on potential anticompetitive behavior by firms within such a group"); Robert Heidt, *Industry Self-Regulation and the Useless Concept "Group Boycott"*, 39 Vand. L. Rev. 1507, (November 1986) (analyzing the antitrust consequences of standard setting organizations); Dennis W. Carlton and J. Mark Klamer, *The Need for Coordination Among Firms, with Special Reference to Network Industries*, 50 U. Chi. L. Rev. 446 (Spring, 1983) (arguing that in spite of potential stifling of competition, coordinated action may be necessary to achieve efficiency). *See also* Sherman Antitrust Act 15 U.S.C. Section 1.

and the music industry. So long as the two can work together on a private standard, they are satisfied to retain the flexibility to quietly hash out its details. But the last time technologists and publishers were unable to agree on standards, the latter sought—and got—legislative fiat to deploy a desired platform in the form of the Audio Home Recording Act of 1992. The AHRA prohibited the "import, manufacture, or distribut[ion of] any digital audio recording device or digital audio interface device that does not conform to … the Serial Copy Management System[,]" which would prevent a copy of material tagged as "not to be copied" from itself being copied.[71]

Standardized architectures of privication may thus be built and wielded by private hands, but their technology is no simple substitute for law: law can readily intervene to bolster or weaken such systems, and might be critical to securing adoption of—if not outright agreement about—the standards that the developers and users will share.

III. Lessons from the publisher: The power of privication architectures

I now review some of the features of trusted privication architectures that make them distinct from law even as they rely upon it. These features allow publishers to control their work more readily than through law alone, and ultimately point to ways that privacy interests can be better vindicated.

[71] *See* 17 U.S.C. 1002(a); Audio Home Recording Act 17 U.S.C 1000-1010; Gary S. Lutzker, *Dat's All Folks: Cahn v. Sony And The Audio Home Recording Act Of 1991 - Merrie Melodies Or Looney Tunes?*, 11 Cardozo Arts & Ent LJ 145 (1992).

A. Discrimination on the basis of consumer characteristics.

Mass publishing has typically by necessity contemplated an undifferentiated market. One cannot distinguish—and the price discriminate—among buyers of intellectual property except in quite crude ways. A publisher might attempt a temporal staging of a new book—the more expensive hardcover edition sold to those who are willing to pay more to buy now, followed by a cheaper paperback edition for those who are more price-sensitive—is a familiar strategy, but the ready transferability of intellectual property eliminates most other schemes of discrimination. Indeed, the first sale doctrine, by which one legitimately encountering a particular copy of a protected work may lend or resell it without restriction, ensures that most serious attempts to distinguish among buyers can be met with arbitrage.[72] Privication can change that, because the systems that enable it can cheaply couple information gathering about a buyer with the quotation of a price, while preventing cheap arbitrage between those who are offered a discount and those who are not. Thus a student gets access to music at a given ongoing rate but cannot readily attain custody of a "copy" of it which in turn may be transferred or simply copied to another person.

B. Nuance in provision of desired information.

With a trusted system, "access" to a work can have a spectrum of meanings far more subtle and powerful than, say, the binary option of either giving someone a compact disc or not. As the hypothetical future of music distribution

described above suggests, unlike traditional publishing, where it is hard to physically dispossess someone of a work after she has bought it, the opportunity to "stream" information—making it available for momentary exposure without giving an actual copy to the consumer—suggests completely new models of information provision with corresponding new metrics of remuneration. A single song can, at the discretion of the publisher, remain a product to be sold and re-sold, or repackaged as a service in which a consumer buys rights to listen to a song for a period of time or a discrete number of plays, after which the rights lapse. Furthermore, songs can be unbundled from one another, no longer forcing publishers to set the boundaries of a given "album."

C. Prevention rather than punishment of undesired behavior.

The effectiveness of traditional "rule and sanction" law as a means of behavior control is a function of its certainty, swiftness, severity, and normative acceptance. The ability of individuals to swap copyrighted music without being readily identified makes the prospect of punishment quite remote, despite a strict law on the books clearly proscribing the act in question. And while it may be difficult to overstate the level of government support for strong intellectual property protection, prosecutorial commitment to expending scarce resources to prosecute individual intellectual property crimes is not likely to be strong; so far only "ringleaders" of intellectual property piracy groups have been targeted. Similarly, though the industry has no reluctance to bring private causes of action

[72] 17 U.S.C. § 109(a) (1999).

against perceived infringers, litigation is costly, time-consuming, and poorly calibrated to the small claims at stake in many instances.

Thus, for that part of the problem that bears on enforcement of constraints against multiple small individuals ("elephant vs. gnats"), a privication framework might be a preferable recipe. If the cost of piracy can be increased through significant barriers to breaking a technical architecture that prevents it, rather than a calculus combining the likelihood of being caught with the severity of punishment, control might be more efficiently effected. Put another way: an ounce of prevention is worth a pound of cure; few banks would prefer a solved robbery to a vault never robbed.

D. "Newtonian" motion: the inertia of trusted systems's constraints.

A well-constructed trusted system could, once established, maintain its constraints comparatively more cheaply and with less government cooperation than those defined and enforced through a legal regime.

A trusted system could be cheaper because, apart from the fixed costs of designing and deploying it, there are low ongoing costs to its maintenance. This is true in the simple sense that software does not wilt after repeated uses, and if its function is to produce sophisticated gates around information, it can continue to staff them without the annuities necessary for human guards. Trusted systems upstage most of law's enforcement mechanisms, dependent as they are on attorneys general, courts, or legislatures.

Moreover, networked technologies can attain a self-perpetuating momentum; once in place they can be quite difficult to uproot.[73] A system intertwining suppliers and consumers exhibits just these network externalities.

The power of market-based network effects reduces the need for continued government backing of the constraint scheme embedded within the network. To be sure, the language used to map out the components and features of a trusted system is the language of law—rights, ownership. These words capture their technical functions while remaining somewhat true to their legal etymology: as with traditional legal rights, they represent the constraints that some users can place on others, constraints from which those others may not readily deviate. Unlike traditional legal rights, however, the constraints designed into most trusted systems—and then invoked by one user against another—are not themselves

[74] Even in the publishing context they are not like copyright, for no legislature defined them, and no court interprets them. They are not like contract, because the assistance of the state is not needed to validate and enforce their terms.[75] They can be at once highly effective and highly independent of government intercession.[76]

---

[73] See generally Brian W. Arthur, Positive Feedbacks in the Economy, 262 Scientific American 92 (1990); Paul David, Clio and the Economics of QWERTY, 75 American Economic Review, 332 (1985); Mark Lemley & David McGowan, Could Java Change Everything?, 520 PLI/Pat 453 (1998).

[74] A "legally protected interest" is a right that is coupled with a duty on other parties not to infringe that right. It is more than a right, in the sense that the courts will use their power to stop the interference with the right. *See* Joseph William Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 Wis. L. Rev. 975, 986-89.

[75] Lawrence Lessig, Code and Other Laws of Cyberspace at 136 ("But contracts are not as bad as code. Contracts are a form of law. If a term of a contract is inconsistent with a value of copyright law, you can refuse to obey it and let the other side get a court to enforce it. The ultimate power of a contract is a decision by a court—to enforce the contract or not. Although courts today are relatively eager to find ways to enforce these contracts, there is at least hope that if the other side makes its case very clear, courts could shift direction again.

This may be an easy feature to miss when reflecting upon the publishing industries' intended use of trusted systems, given how little trouble they have had marshaling government support for ongoing rule-and-sanction protection. Still, even a politically advantaged stakeholder would, all else being equal, presumably wish to rely as little as possible on the possibly fickle solicitousness of the public arena towards its interests.

E. Opportunity for new rights constructs.

The story of trusted systems for publishing so far looks to be one of winner-take-all: the designers of the system tilt each of the features just described to their maximum advantage. In the case of the music industry, we might say that the trustee is computer technology and the companies behind it, and the trusters are ASCAP and BMI. After a rocky start, they are collaborating to ensure that music listeners enjoy their products on the basis of something other than the honor code or the legal code. The untrusted is the public: computer owners at large who might ask their computers to do more with content than the originator of the content would like.

If publishers in a world of trusted privication do not need copyright's protections, its countervailing privileges—already weak—need not be

---

The same is not true of code…Again—where to do we challenge code? When the software protects in a particular way without relying in the end on the state, where can we challenge the nature of the protection? Where can we demand balance when the code takes it away?").

[76] Yochai Benkler, invoking work on "negative liberty," illustrates this distinction quite neatly by pointing out the difference between being "able" to write (or copy) something and being "free" to do so. Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of Public Domain*, 74 N.Y.U. L. Rev. 354, 390 (1999).

respected.[77] Fair use is merely a defense against a claim of copyright infringement; it is not a "right" that one can affirmatively exercise to claim access to data or an ability to copy it. Within the "Trusted Privication" framework, the law's sanctions and exceptions are equally irrelevant, and the issue is only whether the act of copying can be made technically nontrivial.[78]

Because the music industry—the supplier of content—is the predominant force establishing a system of privication, the rights architecture the system reflects might inevitably appear lopsided to consumers of content. This

[77] *See* Cohen, *Lochner in Cyberspace* at 472; Mark Gimbel, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law*, 50 Stan. L. Rev. 1671 (1998).

[78] Analysis of the implications of privication is in its early stages, and no one has yet come up with a thorough theoretical framework to enforce, say, fair use as some sort of "copyduty" right rather than a mere defensive privilege, perhaps expressed as a limitation on what kinds of trusted systems can be deployed. *See* Julie E. Cohen, *A Right to Read Anonymously*, 28 Conn. L. Rev. 981 (1996) 985, ("As justification for the development of digital copyright management systems, copyright owners cite the ease of reproducing and transmitting unauthorized copies of digital works over electronic networks. They argue that technological protection for their works is necessary to prevent widespread infringement, thus giving them the incentive to make their works available online. As the above example suggests however, many copyright owners envision copyright management systems that will be capable of doing far more than simply preventing unauthorized reproduction. One study of existing technologies for copyright management characterizes the ideal technology as "capable of detecting, preventing, and counting a wide range of operations, including open, print, export, copying, modifying, excerpting, and so on."…This vision of the future of copyright management could entail total loss of reader anonymity in cyberspace…It could also entail the demise of the fair use doctrine…However, that is a subject for another article."); Lawrence Lessig, Code and Other Laws of Cyberspace at 137 ("The loss of fair use is a consequence of the perfection of trusted systems. Whether you consider it a problem or not depends on your view of the value of fair use. If you consider it a public value that should exist regardless of the the technological regime, then the emergence of this perfection should trouble you. From your perspective, there was a value latent in the imperfection of the old system that has now been erased."); William W. Fisher III, *Property and Contract on the Internet*, 73 Chi.-Kent. L. Rev. 1203, 1254 (1998) (raising possibility of Congressional authorizing some private intellectual property protection technologies while banning others); Gimbel at 1685-87 (1998) (going so far as to call trusted systems "an invitation to consider whether private ordering is appropriate in the context of intellectual property"); Glenn O. Brown, *Copyduty: Saving Fair Use in the Coming Era of "Privacation*," Student Papers, Seminar on Internet and Society, Harvard Law School, Jan. 1999, available at <http://cyber.law.harvard.edu/is98/final_papers/Brown.html> (exploring the feasibility of implementing a regime of "copyduty," under which fair use would become an affirmative right rather than affirmative defense) (hereinafter, *Copyduty*); Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C.L. Rev. 557, (January, 1998); DanThu Thi Phan, *Will Fair Use Function on the Internet*, 98 Colum. L.

lopsidedness may first appear as simply hyperenforcement of existing intellectual property law.

However, trusted systems and "privication" are not merely about enforcement, and they need not be lopsided. Indeed, they offer opportunities to create new distributions of constraint and freedom among consumer and producer, ones that need not reflect substantively extreme allocations to one or the other. The quite basic trusted system of a taxicab meter enforces a rule on fare calculation, but it also calculates a fare on the basis of subtle combinations of the distance covered and time spent stopped in traffic in a way that driver and passenger simply could not—a new, perhaps "fairer" accounting of what a passenger owes a driver than what a glance at an odometer or reliance on a crude geographic "zone" system could provide.

Some implementations of a trusted system could help better reconcile the conflicting interests of consumers in listening to cheap music (and exchanging ideas and speech with one another) with a level of control over work that would satisfy the music industry. For example, one could imagine allowing "fair use" of music so long as it was not at full digital quality—for example, one could listen freely to songs at AM radio quality, while having to pay to hear them at full fidelity. This might or might not make economic sense to the industry, but in any case it could advance the sort of social policies that underlie fair use by allowing everyone, rich or poor, to benefit from listening to music, without endangering the market for music among those who wish to pay for it. A trusted system might

---

Rev. 169, (January, 1998). Given the trajectory of copyright law's evolution, one might predict that a proposal advancing a copyduty right would not be very welcome in Congress.

provide that elementary school music teachers could play music for their students in the classroom for free, without worry that the students—or teacher—could then take the music home or resell it to others not at school. There could be corresponding new forms of "fair use" for books, articles, speeches, and newspapers. Control might be tightened in some areas, loosened in others.

Unless market forces demand them, these "moderate" systems are unlikely to arise in publishing, at least as long as the industry is building the system and Congress sees no reason to intervene on behalf of the public interest. But these sorts of new balancing constructs may prove quite important for privacy, where privacy advocates are among the least advantaged at the table of public choice.

IV. Medical data: A Trajectory of Personal Privacy Worries—and Responses to Them—in a Digitally Networked Environment

A. A New Problem: Quick, cheap, perfect copies

Sun Microsystems's Scott McNealy laid down the gauntlet to those who care about privacy in the spring of 1999. His observation was pithier than Barlow's declaration to the information industries,[79] if less lyrical:

[79]John Perry Barlow, A Declaration of the Independence of Cyberspace (visited Nov. 27, 1999) <http://www.eff.org/pub/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration> ("Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever

> "You already have zero privacy. Get over it."[80]

The elements of the information technology revolution that worry intellectual property holders carry parallel significance for individuals as personal data holders.[81] After all, whether for profit or dignity, at the core each group desires the same end: control over information. There is, however, a fundamental shifting of roles. In the context of intellectual property, worry has come largely from well-organized corporate interests seeking protection against death by a thousand cuts from "little guy" information pirates. With privacy, worry has come largely from individuals seeking protection against a whittling away of privacy by well-organized corporate interests.[82]

---

the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish").

[80] *See* Edward C. Baig et al., *Privacy: The Internet Wants Your Personal Info. What's in It for You?*, BUSINESS WEEK, Apr. 5, 1999, at 84.

[81] *See* Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 Cath. U.L. Rev. 1183, (1999) ("Fueling online individual privacy concerns is the fact that the collection and use of personal identifiable information have never been cheaper or easier than in the online environment."); Laurie J Flynn, *Privacy Groups 'Honor' Some Institutional Foes*, N.Y. TIMES, Apr. 19, 1999 (describing a mock awards ceremony for notable violations of privacy held at the Computers, Freedom and Privacy Conference); Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 Comm. Law Conspectus 63 (1994) ("The very anonymous nature of the Internet . . . has as much potential for private and governmental abuse as a masked burglar, a con artist, a hooded night rider, or a dossier collecting zealot. The paradox is that in order to protect privacy, anonymity must be limited."); Paul Taylor, *Fears rise over personal privacy: The vast amount of data on the information superhighway is causing concern about the 'Big Brother' age in which we live*, LONDON FINANCIAL TIMES Feb. 4, 1998, at 1 (stating that privacy advocates have "grown so concerned about the sheer volume of data that is now collected about individuals over the internet - much of it available at a price to others - that they are now calling for new a tougher legislation to control the activities of modern-day marketers").

[82] *See* Adam L. Penenberg, *The End of Privacy: Our reporter dared a private eye to dig up dirt on him. The results are terrifying to anybody who worries about prying eyes or credit card scamsters. What can you do to protect yourself?* FORBES NOV. 29, 1999 at 182; Ann Harrison, *Early RealNetworks Slapped With Privacy Lawsuits*, COMPUTERWORLD, Nov. 15, 1999 at 20; Jane Birnbaum, *Here's How To Protect Your Medical Records*, CHICAGO TRIBUNE Nov. 23, 1999 at 1; James Lardner, *Every click you make . . . Shopping online at the office? Your boss may be peeking*, U.S. NEWS & WORLD REP., NOV. 8, 1999 at 69.

More than one commentator has lamented that video rentals are treated to more emphatic federal protection than medical data.[83] This is so despite the rapid digitization of sensitive medical records,[84] a marked increase in the amount of information of which a "medical record" now comprises,[85] and a number of "scare stories" about misuse of medical data.[86]

---

[83] *See* Helena Gail Rubinstein, *If I Am Only for Myself, What Am I?: A Communitarian Look at the Privacy Stalemate*, 25 Am. J. L. And Med. 203, 203 (1999); See note 137, supra on the Video Privacy Protection Act for a full description.

[84] There are several public companies (such as McKesson HBOC, Inc. and IDX Systems Corporation) that provide enterprise IT solutions to healthcare providers, which include electronic medical records management functionalities. Their systems typically do not allow access via the Internet. A provider of client/server medical record management software, MedicaLogic, Inc., has recently developed an Internet-based medical record management application and has filed for an IPO. Major Internet healthcare companies, including drkoop.com, Inc. are also developing Internet medical record management functionalities as part of their offerings. *See* <http://www.drkoop.com/aboutus/products/pmrtour/one.html> (visited Nov. 28, 1999). Numerous startups (MedicalRecord.com and others) have also been trying to enter this market.

[85] *See* Jurevic, at 809-810 (detailing the type of information in a medical record).

[86] *See, e.g.,* Barb Albert, *Patients' medical records inadvertently posted on Net,* THE INDIANAPOLIS STAR, March 30, 1999, at A1 (describing how the "intimate details of some 90 patients' sex lives, along with their names, addresses, phone numbers and credit card numbers, were exposed on the Internet," unbeknownst even to their pychiatrist); Marilyn Chase, *Medical records may be private but they're hardly confidential*, THE SAN DIEGO UNION-TRIBUNE, Dec. 11, 1996, at A26 ("Many people experience unsettling leaks to an employer or the general public about their personal medical information that can be small or life-shattering. It can be something as simple but annoying as having notice of your child's birth given to marketers who release a hail of junk mail promoting baby gear. Or it can be as significant as your company management learning about your past therapy for alcohol abuse."); Douglas Fisher, *Hippocratic Oath for the Information Age*, THE TORONTO SUN, July 29, 1998, at 17 (expressing concern over medical privacy in the digital context and labeling "scary" what the privatization of previously government-run services "has been doing to threaten individuals' privacy"); Jodi Upton, *U-M medical records end up on Web: Patients fear privacy was hurt from mistaken release of names, Social Security numbers,* THE DETROIT NEWS, Feb. 12, 1999 ("Thousands of University of Michigan health system patients had personal and medical information released over the Internet without knowing it, hospital officials said Thursday."); Elizabeth Weise & M.J. Zuckerman, *Balancing acts: Privacy Rights, Internet Access* USA TODAY, Apr. 8, 1999, at 5D ("Americans are increasingly aware of the need to avoid 'a privacy meltdown of Chernobyl-like proportions,' Rep. Edward Markey, D-Mass., said in his keynote address" at the Computers, Freedom, & Privacy Conference in Washington, D.C.); M.J. Zuckerman, *As information flies, privacy could be dead on arrival*, USA TODAY, July 14, 1999, at 4D ("In many instances, sensitive information is being volunteered in . . . inappropriate settings, such as chat rooms and Web pages where patients seek advice or share experiences."); *Safeguards on privacy must be tighter* THE KANSAS CITY STAR, Nov. 3, 1999, at B8 ("For Americans who don't like the idea of having their private medical records opened to indiscriminate scrutiny by curious strangers and companies, one of the most disappointing congressional failures in recent years has been in medical privacy. . . . The abuse of these records can come from unethical health-care organizations, misguided employers and potential employers, sleazy marketing operations and - last but certainly not least - free-lance Peeping Toms.").

B. Solution 1.0: Strengthening medical data privacy rights

Understanding just what is meant by rights over intellectual property is made easier by the existence of Title 17 in the United States and its respective siblings elsewhere.[87] The most politically important sticks within the bundle of rights amounting to "copyright ownership" are specifically and carefully elaborated there,[88] along with generally much vaguer exceptions and reservations.[89] They perhaps have both reflected and perpetuated cultural norms—adjusted for the political weight of various interests—about ownership of one's tangible creative output.

The status quo for privacy has been significantly murkier. The term has taken on varied meanings within and near the general "right to be let alone,"[90] ranging from freedom from humiliating government searches and intrusions[91] to freedom to make personal choices free of government interference,[92] to abilities to control

[87] *See* 17 U.S.C. 101 et seq.; Copyright, Designs and Patents Act, 1988 (United Kingdom); Berne Convention for the Protection of Literary and Artistic Works (Paris Act, 1971); Universal Copyright Convention (195); Melville B. Nimmer & Paul E. Geller, International Copyright Law and Practice, § 3 (1988-94); Jane C. Ginsburg, *Authors And Users In Copyright*, 45 J. Copyright Soc'y U.S.A. 1, Fall, 1997.
[88] *See* 17 U.S.C. § 106.
[89] *See* 17 U.S.C. §§ 107-112. See generally, William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 Harv. L. Rev. 1661 (1988).
[90] *See* Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[91] *See* Michael Adler, *Cyberspace, General Searches, and Digital Contraband: the Fourth Amendment and the Net-Wide Search*, 105 Yale L.J. 1093 (1996).
[92] *See* Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965); John Hart Ely, *The Wages of Crying Wolf: A Comment on Roe v. Wade*, 82 Yale L.J. 920, 930 (1973).

facts (or even falsehoods) linked to oneself.[93] Jerry Kang, in a comprehensive survey of information privacy, reviews these varied definitions and applications, honing in on a distinct meaning of information privacy that triangulates among a scatterplot of sources.[94] Major areas of concern include the transfer of one's personal information by another party to a third for marketing purposes, the publication of embarrassing private personal data, and the use of sensitive personal data by employers and insurance companies in making decisions that might bear heavily on one's economic well-being.[95]

Even if we limit our view of privacy to information privacy, however, there is simply no protection as fully developed in law as Title 17 is for copyright. The information revolution encountered a legal patchwork of information privacy rights that, by any account, is only fitfully mapped out.[96] There are many places where

---

[93] *See* Whalen v. Roe, 429 U.S. 589, 599-600 (1977); Paul v. Davis, 424 U.S. 693 (1976); *see also* William J. Feinrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 Fordham L. Rev. 951(1996).

[94] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998).

[95] *See, e.g.,* Paul Taylor, *Fears rise over personal* privacy, *supra* note 76 (describing consumer fears that personal information will be sold to third parties without the consumer's knowledge); Barb Albert, *Patients' medical records inadvertently posted on Net, infra* note 115 (describing an incident in which over 90 sex therapy patients' intimate data was posted on the Internet); Marilyn Chase, *Medical records may be private but they're hardly confidential*, *infra* note 115 (describing various ways in which embarrassing information might be distributed on the Internet); David Orenstein, *High Standard in Works for Sharing E-Customer Data Ability to easily share information alarms privacy experts, despite planned guidelines*, COMPUTERWORLD, Nov. 22,1999 at 2; Lawrence M. O'Rourke, *News Phone line may be private, but are your records?*, NEWS & OBSERVER, NOV. 7, 1999 AT A1; Richard A Epstein, *Privacy, please*, NAT'L REVIEW, Sept, 27, 1999 at 46; John Schwartz, *IRS Looks to E-Mail as a Tool; Plan to Send Tax Data to Lenders Raises Privacy Concerns*, WASHINGTON POST FINANCIAL, Oct. 23, 1999, at E01; Milt Freudenheim, *Medicine at the Click of a Mouse; On-Line Health Files Are Convenient. Are They Private?* N.Y. TIMES, Aug. 12, 1998.

[96] *See* Erika S. Koster, *Zero Privacy: Personal Data On The Internet* 5 Computer Law. 7 May, 1999 at 9; Jerry Kang*, Cyberspace Privacy: A Primer And Proposal,* 26 Hum. Rts. 3 (Winter, 1999) at 4. There is also much less harmonization of private sector privacy law internationally, especially compared with international intellectual property convention, *see* n. 7 supra. The European Union has adopted a directive mandating that member nations adopt a framework of privacy rights for personal information; no comparable rights exist in U.S. federal law. *See* Jennifer M. Myers, *Creating Data Protection Legislation in the United States: An Examination of*

the U.S. Code defines personal information privacy rights vis-àvis government intrusion.[97] The legislation that is arguably most comprehensive—the Privacy Act of 1974[98]—might have become the "Title 17" of privacy had its proscriptions applied against private actors, as the report from which it drew many of its features recommended.[99]

Current Legislation in the European Union, Span, and the United States, 29 Case W. Res. J. Int'l L. 109 (1997).

[97] Some examples are: Video Privacy Protection Act of 1988 ("VPPA") (18 U.S.C. 2710 (1988)). The VPPA was enacted in response to the revelation, at the Supreme Court nomination hearings of Judge Bork, that a list of his video tape rentals had been procured and made publicly available. The VPPA prohibits video stores from giving third parties information about a customer's rentals or sales. However, mailing lists of customer addresses can be distributed under the VPPA. (18 U.S.C. 2710-2711); The Cable Communications Policy Act of 1984, (47 U.S.C. 551 (1988)) which forbids cable operators and third parties from monitoring the viewing habits of subscribers. (551(c)(2)(C)(ii)(I)); The Fair Credit Reporting Act of 1970 (FCRA) governs the information practices of consumer reporting agencies, such as credit bureaus, and the use of consumer reports and the sharing of affiliate information within bank holding companies and other multicompany organizations. *See* 15 U.S.C.A. 1681-1681u (West Supp. 1998); The Right to Financial Privacy Act of 1978 was enacted as a direct response to the *Miller* decision, and established notice and access procedures for access to financial information by federal government agencies. *See* 12 U.S.C.A. 3401-3422 (West Supp. 1998); The Electronic Fund Transfer Act of 1978 provides a basic framework establishing the rights, liabilities, and responsibilities of parties with respect to electronic fund transfers. Its primary objective is to protect the rights of individuals in such transfers. It also requires notice of the circumstances when account information will regularly be disclosed to third parties. *See* 15 U.S.C.A. 1693-1693r (West 1997); The Cable Communications Policy Act of 1984, as amended by The Cable Television Consumer Protection and Competition Act of 1992, restricts the collection, use and disclosure of information relating to cable systems. *See* 47 U.S.C.A. 551 (West Supp. 1998). The Electronic Communications Privacy Act of 1986 is intended to protect against unauthorized interception of electronic communications. *See* 18 U.S.C.A. 2510-2522 (West Supp. 1998). The Computer Fraud and Abuse Act of 1986 made it a federal crime to "knowingly" access certain computer systems and obtain information without authorization. The intent of Congress was to proscribe intentional acts of unauthorized access and focus federal criminal prosecutions on individuals whose conduct evidenced a clear intent to enter, without proper authorization, computer files or data belonging to a financial institution. *Id*. 1030. The Telephone Consumer Protection Act of 1991 was created to govern telephone solicitations and give the Federal Communications Commission the rulemaking authority to prescribe regulations necessary to protect residential subscribers' privacy by avoiding telephone solicitations to which they object. *See* 47 U.S.C.A. 227 (West Supp. 1998). The Identity Theft and Assumption Deterrence Act of 1998 amended the federal criminal code to make it a crime for a person to knowingly transfer or use, without lawful authority, a means of identification of any other person with the intent to commit, aid or abet any unlawful activity that violates federal law. *See* Pub. L. No. 105-318 , 1998 U.S.C.C.A.N. (112 Stat.) 3007 (to be codified at 18 U.S.C. 1028).

[98] *See* Privacy Act of 1974, 5 U.S.C Section 522(a)

[99] *See* U.S. Department of Health, Education & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973) at xxiii (recommending that individuals be given rights to their own information so that they could take action to protect that information); Priscilla M. Regan, Legislating Privacy, (UNC Press, 1995) (The "bill was comprehensive in its

There are federal laws covering the handling of highly specific and especially sensitive types of collections of personal data in private hands.[100] These include laws governing handling of video rental information,[101] cable subscriber channel preference data,[102] the contents of telephone calls (both landline and cellular),[103] credit reports,[104] financial transactions,[105] and electronic communications generally.[106]

At the state level, some constitutions provide generalized rights of privacy supplemented by interpretive cases,[107] statutes carve out particular privacy interests,[108] and at common law there are threads of tort that have developed for

---

scope, covering all automated and manual personal information systems in federal, state, and local governments as well as the private sector…The compromise bill reflected more of the original House bill in that it covered only federal agencies.")

[100] *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497 (1995); Driver Privacy Protection Act of 1994, 18 U.S.C. 2721 (1994).

[101] *See* Video Privacy Protection Act, 18 U.S.C. § 2710 et. seq.

[102] *See* Cable TV Privacy Act of 1984, 47 U.S.C. § 551.

[103] *See* Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq.

[104] *See* Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681 et seq. (defining the type of consumer information that may be kept, fair practices for disclosure of that information, and remedies for individuals).

[105] *See* Right to Financial Privacy Act, 12 U.S.C. 3401 et seq. (The Right to Financial Privacy Act was Congress' response to a U.S. Supreme Court decision that found bank customers had no legal right of privacy for their financial information held by financial institutions. The law is largely procedural and requires government agencies to provide notice and an opportunity to object before a bank or other institution can disclose personal financial information to a government agency, usually for law enforcement purposes. The law was amended in the latter 1980s to allow postponement of notice in investigations dealing with drug trafficking and espionage)

[106] *See* ECPA, 18 U.S.C. 2510 et. seq.

[107] *See* ILL. CONST. art. I, §§ 6, 12; LA. CONST. art. I, § 5; S.C. CONST. art. I, § 10; ALASKA CONST. art. I, § 22; CAL. CONST. art. I, § 1; MONT. CONST. art. II, § 10; HAW. CONST. art. I §§ 6, 7; FLA. CONST. art. I, §§ 12, 23; WASH. CONST. art. I, § 7; ARIZ. CONST. art II, § 8; Timothy O. Lenz, *"Rights Talk" About Privacy In State Courts*, 60 Alb. L. Rev. 1613 (1997); *Privacy Rights in State Constitutions: Models for Illinois?* 1989 U. Ill. L. Rev. 215.

[108] *See, e.g.* Cal. Penal Code § 637.6 (West Supp. 1991) (protecting personal data gathered by those in the business of organizing car pools); N.J.Stat. Ann. 17:16K-3 (West 1984) (a New Jersey statute permits the disclosure of information relating to electronic fund); Cal. Civ. Code 1748.12 (West 1998) (Cal restricts the disclosure of certain credit card information); Me. Rev. Stat. Ann. tit.9-A, 8-304 (West 1997). *See also,* Robert M. Gellman, *Prescribing Privacy: The Uncertain Role Of The Physician In The Protection Of Patient Privacy*, 62 N.C.L. Rev. 255 (1984) ("There is tremendous variation in the number and quality of state laws on medical confidentiality. A 1979 review by the National Commission on Confidentiality of Health Records (NCCHR) of

misuse of personal information since Warren and Brandeis's famous call for such actions over a century ago.[109]

Without weighing in on the comparative substantive importance—either to the principals involved or to society generally—of enabling control over respective types of information, a coarse comparison of the intellectual property and privacy protection regimes suggests that the former was and is more securely protected under law.

This differential is even more striking when the transposition of parties is taken into account between the two areas. Intellectual property stakeholders have a direct economic calculus by which to measure and justify the amount of protection to insist upon, whether through private causes of action[110] under expanding copyright law,[111] enforcement of contracts that bear on control,[112] or funding the development and deployment of technological self-help schemes.[113] As noted earlier, some of the most prominent stakeholders are themselves collective organizations that can apply economies of scale in the processes of

---

laws on the maintenance, use, and disclosure of personally identified patient information found that Vermont had seven such laws, but that Hawaii had thirty-nine"); Joy Pritts, Janlori Goldman, Zoe Hudson, Aimee Berenson, and Elizabeth Hadley, *The State of Health Privacy: An Uneven Terrain/A Comprehensive Survey of State Health Privacy Statutes,* Health Privacy Project, July 1999, (visited Nov. 28, 1999) <http://www.healthprivacy.org/resources/statereports/keyfind.html> (describing the extent and variation between states protections of health information).

[109] *See* Warren & Brandeis, *The Right to Privacy*; William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960); RESTATEMENT (SECOND) OF TORTS 652A-652E (1977). For a more recent overview with attention to information technology, For a more recent overview with attention to information technology, *see* Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 Tex. L. Rev. 1395 (1987); *see generally* William J. Fenrich, *Common Law Protection of Individual's Rights in Personal Information*, 65 Fordham L. Rev. 951 (1996).

[110] 17 U.S.C. 501-505;17 U.S.C.S. § 501(b) (1999).

[111] See text accompanying notes 17-21 *supra*.

[112] See text accompanying notes 30-35 *supra*.

[113] See text accompanying notes 62-83 *supra*.

expanding and defending the reach of intellectual property rights, including the investigation and prosecution of particular infringements.[114]

---

[114] *See* American Society of Composers, Authors and Publishers (visited Nov. 28, 1999) <http://www.ascap.com> (home page), (visited Nov. 28, 1999) <http://www.ascap.com/about/about.html> (about ASCAP) ("ASCAP is the American Society of Composers, Authors and Publishers, a membership association of over 80,000 composers, songwriters, lyricists and music publishers. ASCAP's function is to protect the rights of its members by licensing and paying royalties for the public performances of their copyrighted works"); Recording Industry Association of America (visited Nov. 28, 1999) <http://www.riaa.com/about/aboutus.htm> (about RIAA) <http://www.riaa.com/> (home page) ("The Recording Industry Association of America is the trade group for the recorded music you enjoy every day. Our members are the companies that comprise the most vibrant national music industry in the world. Our mission is to foster a business and legal climate that supports and promotes our members' creative and financial vitality around the world"); Software Publisher's Association and Software & Information Industry Association (visited Nov. 28, 1999) <http://www.siia.net/> (home page) (visited Nov. 28, 1999) <http://www.siia.net/piracy/programs/backgrounder.htm> (SPA anti-piracy mission statement) ("The Software & Information Industry Association's SPA Anti-Piracy Division conducts a comprehensive, industry-wide campaign to fight software piracy. The pro-active campaign is premised on the notion that one must balance enforcement with education in order to be effective. The campaign has two broad charters: educate users about the copyright law and provide them with information necessary to comply with it, and Enforce members' copyrights and trademarks. SPA Anti-Piracy's efforts are conducted on behalf of any SIIA member who wants to be involved. Currently, over 90 percent of SIIA member companies are involved in the anti-piracy campaign. The campaign is successful because organizations that pirate software steal from all software publishers, not just one or two. This makes SIIA's SPA Anti-Piracy program very valuable as organizations are required to "come clean" on all member software. The program began in 1985 under the direction of the Software Publishers Association (SPA) which merged with the Information Industry Association in January 1999 to form the Software & Information Industry Association (SIIA)"); Association of American Publishers, (visited Nov. 28, 1999) <http://www.publishers.org/2.htm> (home page) (visited Nov. 28, 1999) <http://www.publishers.org/home/issues/index.htm#copyright> (copyright page) ("Publishers in the United States and worldwide are facing enormous challenges in the area of intellectual property protection. Securing copyrighted works against unauthorized use in print and electronic format, in the domestic and international marketplace; protecting the integrity of copyrighted works in the digital environment; tracking the use of these works; and developing workable compensation mechanisms are essential if the industry is going to survive and grow. The AAP is devoting significant resources to meeting this challenge"); Broadcast Music, Inc., home page (visited Nov. 28, 1999) <http://bmi.com/>; Motion Picture Association of America, home page (visited Nov. 28, 1999) <http://www.mpaa.org/> (visited Nov. 28, 1999) <http://www.mpaa.org/about/> (about MPAA) ("The Motion Picture Association of America (MPAA) and its international counterpart, the Motion Picture Association (MPA) serve as the voice and advocate of the American motion picture, home video and television industries, domestically through the MPAA and internationally through the MPA"); National Music Publisher's Association, home page (visited Nov. 28, 1999) <http://www.nmpa.org/> (visited Nov. 28, 1999) <http://www.nmpa.org/nmpa.html> (about NMPA) ("Since 1917, NMPA has been a strong and effective champion for the protection of music copyrights in an age of rapid technological changes. NMPA was a leading voice for music publishers in connection with the enactment of the Copyright Act of 1976, and has successfully advocated amendments to that Act where necessary to protect the interests of music copyright owners"); Songwriter's Guild of America, home page, (visited Nov. 28, 1999) <http://www.songwriters.org/>; *see also* Recording Indus. Ass'n v. Diamond Multimedia Sys. Inc 180 F.3d 1072, 1999 WL 387265 (9th Cir. 1999).

The privacy-seeking individual is, by contrast, far less well equipped to assert her information "rights."[115] The Federal Trade Commission can rarely take on individual privacy violations alleged to rise to the level of unfair trade practices, focusing instead on violations that seem widespread and systematic.[116] For an individual to bring a lawsuit for, say, invasion of a common law right such as that against "misappropriation of personal data,"[117] is simply not as easy as it is for a record company to pursue a pirate; the nature of the right makes for a less mechanical cause of action, and the aggrieved plaintiff may be fighting for dignity more than any likely remuneration.[118] As for contract rights, alleged invaders of privacy may not have contractual privity with invadees, and where privity exists

---

[115] *See e.g.,* Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age?"* 25 Wm. Mitchell L. Rev. 223 (1999) ("Right now, the way we currently protect the privacy of our medical records is erratic at best--dangerous at worst. It is time for our nation to enact federal legislation to protect the age-old right to privacy in this new world of progress.'" and "…[T]he current complex patchwork of federal and state protections is insufficient in this age of information technology. Comprehensive federal legislation will be required to meet the challenge of maintaining the confidentiality of individually- identifiable medical information, while still making appropriate information available for necessary and valuable public uses."); Scott Burris, *Healthcare Privacy & Confidentiality: The Complete Legal Guide*, 16 J. Legal Med 447, 451 (1995) ("the only reasonable expectation of privacy is no expectation of privacy at all.") (reviewing Jonathan P. Tomes, Healthcare Privacy & Confidentiality: The Complete Legal Guide (1994)). ("Privacy doctrine today is largely devoted to perpetuating a myth--a myth of "privacy rights' in which autonomous individuals are capable of exercising actual control over information that is to be found in the minds or papers of identifiable individuals.") *Id*.

[116] *See* Federal Trade Commission, *Where to Go for More Information*, (visited Nov. 29, 1999) <http://www.ftc.gov/ftc/moreinfo.htm> ("Letters from consumers are very important to the work of the FTC. They are often the first indication of a problem in the marketplace and may provide the initial evidence to begin an investigation. If you have a consumer problem or complaint, write to the Federal Trade Commission. Although the agency cannot act to resolve individual problems, it can act when it sees a pattern of possible law violations develop.")

[117] *See* RESTATEMENT (SECOND) OF TORTS 652A-652E (1977); Warren & Brandeis, *The Right to Privacy*.

[118] *See* Avrahami v. U.S. News & World Rep., Inc., No. 96-203, slip op. (Cir. Ct. Arlington County June 13, 1996), *cited in* William J. Fenrich, *Common Law Protection of Individual's Rights in Personal Information*, 65 Fordham L. Rev. 951 (1996) (in which plaintiff objected to defendant's selling of his name and address to a third party for marketing purposes, losing because he had intentionally misspelled his name in order to track its sale); Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 Cornell L. Rev. 1756 (1995) ("As applied by the courts, none of these torts offers more than minimal assistance

the "little guy" worried about privacy may be the weaker party in the contract, unable *ex ante* to readily negotiate, afford, or even rationally account for privacy protection that truly reflects his or her preferences, particularly when the use of personal information is ancillary to the transaction in question.[119] For example, few people would be in a position to dwell upon what will happen to data about their car rental as they present their drivers' licenses, sign a few forms, and pick up their keys.[120]

The interests that are well organized to protect copyright are among the commercial interests who fight any movement towards strong privacy legislation, fearing it will interfere with personalized marketing efforts. Indeed, the very music and technology industries that are building structures to defend their control over artistic data are building personal data collection and use mechanisms into those structures.[121] This may explain why the few existing explicit federal privacy protections are as narrow as the exceptions to copyright in

---

to a consumer who claims that a credit bureau's collection or disclosure of personal information

[119] Consumers are clearly ambivalent in their views about privacy. On one hand there is ample data demonstrating intense concern; *compare* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1196-98 (1998) (discussing various surveys, each eliciting strong and increasing consumer concern for personal privacy, and describing public outrage upon discovery of certain personal information-selling practices); *with* Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1 ("Most Americans … are willing to part with personal information as long as they get something in return, and as long as they know what is to be done with the information. They are happy to carry supermarket discount cards. They are annoyed when they get new computers and must re-enter all the information needed for one-click ordering at Amazon.com."). However, Hafner does note that "[t]hese same people, however, are highly protective of their medical records and are generally appalled when they learn of clandestine data collection practices." *Id.*

[120] *But cf.* Shorr, n. 118 *infra*, expressing confidence in a privacy contracting regime at least for credit bureau data. ("[A]n alternative legal regime grounded in property and contract law can protect privacy from credit bureau invasions without unreasonably infringing free commercial speech.")

[121] *See* Ann Harrison, *RealNetworks Slapped with Privacy* Lawsuits; Hilary Rosen (President & CEO,Recording Industry Association of America), *Testimony*, House of Representatives

the Fair Music Licensing Act; some were passed in response to specific privacy "crises," and they all faced intense lobbying to narrow their scope before passage and intense litigation to cabin their scope after passage. For example, the 1994 Drivers Privacy Protection Act was passed only in response to the stalking of Rebecca Schaefer, a well-known actress; it remains the subject of litigation.[122] The Video Rental Act was passed after the release of Judge Robert Bork's video rental information during confirmation hearings on his nomination to the Supreme Court; before passage, the measure was trimmed back to ensure that video rental stores could still sell customer lists.[123] The Privacy Act is credited to Watergate, and as mentioned the private sector was exempted from its proscriptions after industry weighed in.[124] In essence: rational, profit-maximizing industry quite naturally works to maintain a legal framework through which it can control its own information while trafficking freely in the information of individuals. Whatever privacy's value or popularity as an abstract concept, attempts to legislate it are met with stiff resistance far more organized than the forward momentum generated by individuals who covet it.[125]

Commerce Telecommunications, Trade and Consumer Protection, October 28, 1999, 1999 WL 988372 (F.D.C.H.)

[122] *See* Driver's Privacy Protection Act of 1994 ("DPPA") (Pub. L. No. 103-322,108 Stat. 1766, 2099-2102 (codified at 18 U.S.C. 2721-2725) (1994)); Thomas H. Odom, Gregory S. Feder, *Challenging the Federal Driver's Privacy Protection Act: The Next Step in Developing a Jurisprudence of Process-Oriented Federalism Under the Tenth Amendment*, 53 U. Miami L. Rev. 71, n. 2 (1998); Jane E. Kirtley, *Data Protection Law and the European Union's Directive: the challenge for the united states the EU data protection directive and the first amendment: why a "press exemption" won't work*, 80 Iowa L. Rev. 639.

[123] *See* Regan, at 207.

[124] *See* Regan, cf 139.

[125] For a thorough treatment of this phenomenon, *see* Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press: 1995) at 181-211.

Whatever the difficulties of using existing legal tools to solve privacy problems, privacy advocates have had little else in their arsenal to combat the loss of privacy brought on by the information revolution. Federal legislation to protect medical information has been repeatedly proposed.[126] To date, none has passed,[127] though many states have relevant statutes in place.[128]

Congress formally punted on the issue in 1996 when it passed the Health Insurance Portability and Accountability Act.[129] The Act's "administrative simplification" provisions were intended to assist the health care industry in standardizing electronic formats for medical records, ultimately by having the government mandate certain technical standards derived from the private sector.[130] Some standards have already been generated through this process.[131]

---

[126] Proposed medical privacy legislation includes: Federal Privacy of Medical Information Act (H.R. 5935) (1977); Fair Health Information Practices Act of 1994 (H.R. 4077); Health Security Act (H.R. 3600) (1993-94); Health Insurance Portability and Accountability Act of 1996; Health Care Personal Information Nondisclosure Act of 1998 (S. 1921); and the Consumer Protection and Medical Record Confidentiality Act of 1998. See Regan at 105-106. Medical Records Confidentiality Act of 1995, S. 1360, 104th Cong., 1st Sess (1995); *See* Judith Beth Prowda, *A Lawyer's Ramble Down the Information Superhighway: Privacy and Security of Data*, 64 Fordham L. Rev. 738 (1995).

[127] *Id* at 755.

[128] Robert M. Gellman, *Prescribing Privacy: The Uncertain Role Of The Physician In The Protection Of Patient Privacy*, 62 N.C.L. Rev. 255 (1984) ("There is tremendous variation in the number and quality of state laws on medical confidentiality. A 1979 review by the National Commission on Confidentiality of Health Records (NCCHR) of laws on the maintenance, use, and disclosure of personally identified patient information found that Vermont had seven such laws, but that Hawaii had thirty-nine"); Joy Pritts, Janlori Goldman, Zoe Hudson, Aimee Berenson, and Elizabeth Hadley, *The State of Health Privacy: An Uneven Terrain/A Comprehensive Survey of State Health Privacy Statutes*, Health Privacy Project, July 1999, (visited Nov. 28, 1999) <http://www.healthprivacy.org/resources/statereports/keyfind.html> (describing the extent and variation between states protections of health information).

[129] *See* Public Law 104-191. Full text available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ191.104> (last visited 27-Nov-99). Legislative information available at <http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR03103:|TOM:/bss/d104query.html|> (last visited 27-Nov-99).

[130] *See* 42 USCA § 1320d-2 (1999); "Summary of Proposed Standards for Privacy of Individually Identifiable Health Information" available at <http://aspe.os.dhhs.gov/admnsimp/pvcsumm.htm> (last visited 27-Nov-99).

[131] Pub. L. 104-191 TITLE II--PREVENTING HEALTH CARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM, Part C--Administrative

The law also set an August 1999 deadline for Congress to come up with privacy restrictions to go along with the technical standards for electronic medical records.[132] Congress missed its deadline, and the law requires as a result that the Secretary of Health and Human Services shall impose such standards in its stead by February 2000.[133] The Secretary's draft regulations were put out for public comment in November 1999.[134]

Simplification, SEC. 1172(c)(3) at <http://aspe.hhs.gov/admnsimp/pl104191.htm#1172> says: 3) CONSULTATION REQUIREMENT.-- "(A) IN GENERAL.--A standard may not be adopted under this part unless-- "(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and "(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f), consulted with each of the organizations described in subparagraph (B) before adopting the standard. "(B) ORGANIZATIONS DESCRIBED.--The organizations referred to in subparagraph (A) are the following: "(i) The National Uniform Billing Committee. "(ii) The National Uniform Claim Committee. "(iii) The Workgroup for Electronic Data Interchange. "(iv) The American Dental Association. There have been four sets of standards approved. See <http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=14> I looked at the Standards for Electronic Transactions and Code Sets and it appears that these fell under (3)(A)(i) (in that it was the work product of an existing standard-setting organization). A complex internal review process was developed which included consultation with industry as well as a public comment period.

[132] *See* Pub. L. 104-191 § 264(c)(1). "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act … is not enacted by the date that is 36 months after the date of the enactment of this Act (Aug. 21, 1996), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act." Contained in annotations to 42 USCA § 1320d-2 (1999).

[133] *Id*.

[134] *See Notice of Proposed Rule Making for Standards for Privacy of Individually Identifiable Health Information* available at <http://www.hhs.gov/hottopics/healthinfo/index.html> (last visited 28-Nov-99, herinafter Proposed Rules). *See also* 45 CFR Parts 160 Through 164, *Standards for Privacy of Individually Identifiable Health Information; Proposed Rule*, November 3, 1999. (alternative format: Federal Register / Vol. 64, No. 212 / Wednesday, November 3, 1999 / Proposed Rules, pp. 59917-60065); *Summary of Proposed Standards*, n106 supra.

125 42 USC § 1320d-6. "(a) Offense
A person who knowingly and in violation of this part--
(1) uses or causes to be used a unique health identifier;
(2) obtains individually identifiable health information relating to an individual; or
(3) discloses individually identifiable health information to another person,
shall be punished as provided in subsection (b) of this section.
(b) Penalties
A person described in subsection (a) of this section shall--
(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
(2) if the offense is committed under false pretenses, be fined not more than $100,000,

The draft regulations entail substantive enhancements to privacy rights combining the fiat of rule-and-sanction regulation[135] with a dash of strengthened contract-like rights.[136] For example, health organizations may not release medical records that are easily identifiable unless certain specific exceptions apply.[137] Further, patients are given the right to inspect their own records.[138] No private right of action is contemplated for violation of any of the rule's proscriptions.[139] Identifiable data may be released for virtually any otherwise-lawful purpose with a patient's consent, and the rule goes into great detail about how that consent should be obtained, featuring a number of mandatory disclosures and a requirement that the consent be revocable.[140]

At least one health privacy watchdog group has gone on record as being generally pleased with the regulations, noting that in several areas they protect privacy as much as the discretion granted by Congress to HHS allowed.[141] Still, read in light of the copyright analysis discussed above, they reflect the institutional disparities guarding the respective interests at stake. A "copyright"

---

imprisoned not more than 5 years, or both; and
(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both." See also "Summary of Proposed Standards," n106 supra. See also § 164.506(a) and § 164.510 *et. seq.* of Proposed Rules, n109 supra. See also Latanya Sweeney, Weaving Technology and Policy Together to Maintain Confidentiality, 25 J.L. MED. & ETHICS 98, 100 (1997). (Notes: Sweeny article not available electronically, is this the correct article?).

[135] See section II.A.

[136] See section II.B.

[137] See note 169, supra. *A.2. Covered Information* (visited Nov. 29 1998) <http://www.hhs.gov/hottopics/healthinfo/pvc06.htm>("We propose to apply the standards in this proposed regulation to individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity, including such information when it is in non-electronic form (e.g., printed on paper) or discussed orally.")

[138] See note 169, supra. Right of access for inspection or copying. (§ 164.514(a))

[139] See note 169, supra. Rights of individuals (§§ 164.512 - 164.516)

[140] See note 169, supra. (Uses and disclosures with individual authorization. (§ 164.508))

[141] *See* <http://www.healthprivacy.org/latest/RegSum.fin.html>.

regime of rights for privacy would entail an explicit statement of exclusive rights given the patient, with a few specific carve-outs for the purposes of "fair use," which would be quite vague and difficult for fair users to rely upon.[142] Instead of establishing "privacyright," however, the regulations merely subject identifiable medical data to "fair information practices"—the sort of protection identified by at least one scholar as a consistent means of undermining a sold rights regime.[143] These practices are standards rather than rules, requiring that the covered entities "not use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose."[144] Under the rubric of "scalability," the HHS draft considers implementation of these rights to be "flexible," asking each covered entity to "assess its own needs and implement privacy policies appropriate to its information practices and business requirements."[145] The carve-outs are, by comparison, quite explicit, allowing law

[142] While a regime of clear rule cabined by exceptions expressed as vague standards need not always harm those seeking to invoke the exceptions, the case-by-case basis on which courts decide fair use claims, and the ability of the rights holder to choose when and whether to bring an action, make individual users of copyrighted material legitimately uncertain about the scope of the privileges they enjoy. See generally, William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 Harv. L. Rev. 1661 (1988).

[143] *See* Regan at 178.

[144] See note 169, supra ("Covered entities also would be permitted to use or disclose an individual's protected health information for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners. Covered entities would be permitted by this rule to use and disclose protected health information when required to do so by other law, such as a mandatory reporting requirement under State law or pursuant to a search warrant. See proposed § 164.510. Covered entities would be required by this rule to disclose protected health information for only two purposes: to permit individuals to inspect and copy protected health information about them (see proposed § 164.514) and for enforcement of this rule (see proposed § 164.522(e)).")

[145] *See* U.S. Department Of Health & Human Services, *Proposed Standards for Privacy of Individually Identifiable Health Information* (visited Nov. 29, 1999) <http://aspe.os.dhhs.gov/admnsimp/pvcsumm.htm>; note 180, supra. For a critique of distributed emergence of fair information practices, *see* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497, 511 (1995) ("The pursuit of targeted standards at a time of explosive growth in wide-scale information processing activity makes the actual determination of rights, responsibilities, and practices in American society

enforcement, medical research, and other government interests continued access to patient records without consent, so long as certain procedural steps are followed.[146] HHS may ultimately exact civil penalties for violation of its privacy rules, and in some cases may refer privacy violations to the Department of Justice for criminal prosecution. However, its own proposed regulations treat both of these actions as last resorts, preferring "informal resolution" on a case-by-case basis to more formal and precedent setting procedures that could have a deterrent effect.[147] As with my analysis of copyright, I do not here mean to analyze whether these carve-outs are good public policy; rather, I wish to underscore the levels of specificity and enforceability—and therefore "usability"—at which the rights and exceptions are expressed, seen in light of the political power of the interests behind each.

How much of a difference the proposed rules might make for privacy is difficult to predict, especially when one considers the backdrop of enhanced portability of electronic records that the HIPAA hastens.[148] As the November

---

complex. The varied standards for fair information practice offer overlapping, yet distinct, treatment of personal information. Only the combination of legal rules, industry norms, and business practices can properly define the scope of standards for the treatment of personal information in the private sector.")

[146] See note 169, supra. (§ 164.510(b)-(n)); See generally, William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 Harv. L. Rev. 1661 (1988).

[147] *See* <http://aspe.os.dhhs.gov/adminsimp/nprm/pvc49.htm>.

[148] Relationship to State laws at <http://aspe.os.dhhs.gov/admnsimp/nprm/pvc47.htm>; Sec. Pub. Law 104-191 Sec. 1178. Effect on State Law at <http://aspe.os.dhhs.gov/admnsimp/pl104191.htm#1178 264(c)(2)> at <http://aspe.hhs.gov/admnsimp/pl104191.htm#264> PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation. See text at http://aspe.os.dhhs.gov/admnsimp/nprm/pvc47.htm

"Section 264 of HIPAA contains a related preemption provision. Section 264(c)(2) is, as discussed above, an exception to the "general rule" that the federal standards and requirements preempt contrary State law. Section 264(c)(2) provides, instead, that contrary State laws that relate to the privacy of individually identifiable health information will not be preempted by the

draft would have it, there is no private right of action for violations of the regulations. Thus ongoing enforcement by government agencies and prosecutors will be needed to guarantee respect of the new rights. Further, how genuine patients' consent will prove to be—which, once granted, permits the data free-for-all to continue—is also difficult to predict, although the regulations do prohibit the conditioning of medical care on consent to data sharing.[149]

There are other possible legal approaches to solving the medical privacy problem in the era of promiscuous publication. In one approach, Congress could enable aggrieved citizens to bring class actions representing individuals whose privacy rights have been violated, thereby discouraging misuse of medical records. Of course, with the records in custody of the defendant and the information within possibly available from other sources, those whose privacy has been violated often have no way of knowing of the fact of the violation—much less the source. Junk mail from a vitamin supplements company may be random or may be targeted based on records drawn from cancer sufferers. A denial of employment might be based on a bad interview or on knowledge that the applicant is HIV-positive. Furthermore, a class action regime is essentially reactive rather than preventive—at least for the current round of plaintiffs. Money damages may be better than nothing, and they might help reduce future privacy violations, but the patient might well prefer that the violation never happened to

---

federal requirements, if they are "more stringent" than those requirements. This policy, under which the federal privacy protections act as a floor, but not a ceiling on, privacy protections, is consistent with the Secretary's Recommendations."

[149] *64 FR 59918, Vol. 64, No. 212, Proposed Rules, DEPARTMENT OF HEALTH AND HUMAN SERVICES, (HHS) Section 164.506(a) Use and Disclosure for Treatment, Payment, and Health Care Operations*. "We also propose to prohibit covered entities from seeking individual

begin with. Finally, potential industry defendants would likely bitterly oppose such a system because it introduces an element of uncertainty into their choices of what to do with the medical information they ward.

A second approach could be to create a general privacy right with respect to medical records along with a safe harbor provision for those who wish to use medical data. A safe harbor provision generally sets up a set of standards with which an entity can comply in order to ensure freedom from legal liability. It functions as an incentive to behave responsibly.[150] Use of safe harbors in the information privacy context has recently become an issue in the United States in response to the European Union's directive on information privacy.[151] Since the

---

authorization for uses and disclosures for treatment, payment and health care operations unless required by State or other applicable law."

[150] Safe harbors are already used by the SEC in the context of corporate disclosures and by the EPA in the context of environmental preservation; see Private Securities Litigation Reform Act of 1995, H.R. 1058; "Announcement of Final Safe Harbor Policy" EPA (last visited 2/19/2000) at <http://www.epa.gov/fedrgstr/EPA-SPECIES/1999/June/Day-17/e15256.htm>.

[151] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). *See also,* Presidents Information Infrastructure Task Force, "Options for Promoting Privacy on the National Information Infrastructure" (April 1997) (last visited 2/19/2000) at <http://www.iitf.nist.gov/ipc/privacy.htm#N_9_> ("Under the EU Directive, personal data must be collected for specified and legitimate purposes and "not processed in a way incompatible with those purposes." Data must be adequate, relevant, accurate, current, not excessive, and must not be kept in identifying form for any longer than necessary. Personal data may be processed only if the data subject has consented "unambiguously" or if the processing falls within an exception, some of which include contract, legal obligation, or where a data subject's "fundamental rights and freedoms" in the personal information do not outweigh the legitimate interests of the data gatherer and where processing is necessary to pursue these interests. Under the EU Directive, member states must provide judicial remedies for any breach of the rights guaranteed, and adopt enforcement mechanisms, including sanctions for infringements of the privacy laws enacted in conformance with the Directive. The EU Directive requires member states to establish supervisory authorities to monitor the application of national law adopted pursuant to the EU Directive. The supervisory authorities are required to have investigatory authority, effective powers of intervention, and the power to engage in legal proceedings or to bring violations to the attention of judicial authorities. Article 25(2) of the EU Directive requires member states to ensure that personal data is transferred only to third countries with "adequate" privacy protection. Adequacy is to be determined on a case by case basis in light of all the circumstances surrounding a particular data transfer. The U.S. and EU are discussing how the EU Directive might affect transatlantic data flow, but these discussions are in early stages. Nevertheless, no discussion of online privacy protection can be complete without

EU began requiring certain privacy guarantees for participation in information exchange, the United States government has been working to negotiate a safe harbor provision that would help U.S. entities both know what they needed to do to comply as well as avoid liability.[152] Certain privacy advocates have lauded this approach.[153] This is a promising approach, but still requires an enforcement mechanism that might fall short.

The elephants of the music industry found it easy to bend law to their interests, but still unfulfilling because it is a difficult tool to employ against the individual gnats that would flout it. Privacy advocates may face roughly the inverse problem: they will find law more difficult to bend to their interests, since they face more organized and powerful opposition to the creation of clear, substantive rights. Moreover, while the elephants who wish to consume and share data in the medical privacy context may be more responsive to the prod of legal enforcement than their individual counterpart consumers in copyright, it may be harder for the individuals who are sources of medical data to engage the corresponding mechanisms of enforcement. Even the HHS regulations—drafted by policymakers quite sympathetic to privacy interests—couple formal enforcement teeth with paeans to "flexibility" for those charged with guarding privacy and a desire for "informal resolution" above rule and sanction.

---

appropriate consideration of the EU Directive and its implications for international trade in the Information Age.")

[152] *See* U.S. Department of Government, "Draft International Safe Harbor Privacy Principles" (November 15, 1999) (last visited 2/19/2000) at <http://www.ita.doc.gov/td/ecom/Principles1199.htm>.

C. Solution 2.0: Technological self-help through trusted systems

A patient's record and a musician's record may appear quite different to the casual observer, but as we have seen, both boil down to data susceptible to an Era of Promiscuous Publication, harming the interests of their respective owners.[154]

As the music industry is discovering—enough so that its former horror over the Internet is giving way to an embrace—it can seek to protect against technology's perceived excesses by having the desired limits themselves be of technological character, embedded in the very scheme thought to be causing the potential for abuse.

Consider three of the interrelated new rights proposed in the HHS draft regulations: a patient's right to inspect his or her information in a medical database, a patient's right to give consent before that information is transferred for many purposes, and a patient's right to receive an accounting of instances in which information has been disclosed.[155]

As we have seen, while the original Act's administrative simplification provisions are intended to bring about easier information sharing among holders of medical data through quite thoroughly elaborated technical standards—which

---

[153] *See* Phil Agre, "EU/US Privacy Safe Harbor", Red Rock Eater News Service, (1998) (last visited 2/19/2000) at <http://www.tao.ca/wind/rre/0572.html>.
[154] *See* note 13, supra. (David Post)
[155] *See* §§ 164.514(a) and 164.515 of Proposed Rules, n109 supra; *Summary of Proposed Standards* n.106 *supra*; *Summary and purpose of the proposed rule of Proposed Rules*, n.109 supra.

makes an invasion of privacy easier[156]—the accompanying privacy rights implementations float at a much higher level of abstraction, variable from one entity to the next in the name of "flexibility."

For example, a hospital with a highly efficient electronic records scheme could nonetheless insist on fulfilling the patient's right to inspect data or gain an accounting of its redistribution by requiring the filling out of a paper form, performing a less-than-instantaneous manual search, and then releasing photocopied sheets in fulfillment of the request.[157] Indeed, this is just how the "Medical Information Bureau" clearinghouse—a Massachusetts company that gathers and redistributes health data on fifteen million Americans for insurance assessment purposes—currently allows patients to review the records accumulated on them.[158] After the request is fulfilled, a new cycle of paperwork would presumably be necessary to see updates to one's data.

---

[156] "Presumably, authorized users of health information would possess a patient identification number that would grant them access to all or part of the electronic record. The unique identifier would permit entry to many potential data sources held by government agencies, heath plans, health data organizations, and other information holders. If follows that physicians, nurses, pharmacists, lab technicians, administrators, payors, regulators, and many others could retrieve a comprehensive health record from any geographic area linked to the health data network. Patients would not consent to access other than in the most general way, and could not realistically govern the manner in which data were utilized." Lawrence O. Gostin, *Health Information Privacy*, 80 Cornell L. Rev. 451, 485.

[157] If the response rates for FOIA are any indicator--and, to be sure, a healthcare institution is not a government agency--weeks-long turnaround times even for electronic records would not be unsurprising. *See* Don J. Benedictis, *LOGJAM BREAKUP: Court Ruling Could Speed Freedom of Information Requests*, 75 A.B.A.J. 28, (September, 1989); Christopher Dorobek, *Agencies Lag in E-FOIA efforts*, GOVERNMENT COMPUTER NEWS, January 12, 1998, at 1.

[158] MIB home page (visited Nov. 28, 1999) <http://www.mib.com/> (visited Nov 28, 1999) <http://www.mib.com/consumer/about_general.html> (About MIB) The MIB website states that it complies with requests for disclosures within 30 days. Bruce L. Watson, *Disclosure of Computerized Health Care Information: Provider Privacy Rights Under Supply Side Competition*, 7 Am. J. L. and Med. 265, (1981) , Sandra Byrd Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 Fed. Comm. L.J. 163 (1995) ("An insurance company can combine this information with medical records that can be obtained from the Medical Information Bureau (MIB) which has data on 15 million people. The result is a very complete picture of a person's lifestyle, regardless of whether or not the information is

Similarly, consent for redistribution of data might be obtained through a stylized exchange of paper at the initiation of the relationship between a patient and an entity covered by the regulations. While the regulations insist upon a thorough disclosure to the patient of the intended uses of information being collected or generated, including an explicit statement of intention to sell or barter the information,[159] it appears that a blanket authorization can be obtained once and never revisited unless the patient seeks to do so, presumably through another flurry of paperwork. While this may not satisfy privacy advocates,[160] any stronger rendering of consent—for example, requiring assent for each non-medically-necessary release of identifiable patient data—raises transaction costs on the releaser that do not satisfy others.[161]

Finally, whatever the legal rules about privacy, an *un*trusted (in the technical sense) implementation of whatever information-sharing standards emerge from

---

accurate. Furthermore, although the information collected concerns some of the most intimate details of personal life, individuals may be unaware of its existence and, therefore, unable to correct any misinformation contained in these records").

[159] *See* § 164.512 of Proposed Rules, n109 supra, "we would require covered plans or providers to develop and document policies and procedures relating to use, disclosure, and access to protected health information."; § 164.520 of Proposed Rules, n109 supra.

[160] *See e.g.*, *Some Groups Cool to New Privacy Rules, Insurance, Rights Leaders Complain*, SEATTLE POST-INTELLIGENCER, Oct. 30, 1999 ("'We question why it takes over 600 pages to provide medical records confidentiality protection when it took our Founding Fathers only one page to provide Americans with all their basic rights,' said Mary Nell Lehnhard, senior vice president at the Blue Cross and Blue Shield Association." And, "The police should not be able to say to a hospital: 'Give us Mr. Smith's medical charts because we think something's fishy,' said ACLU legislative consultant Ronald Weich. 'One of the most basic principles of American justice is that police must obtain a warrant from a judge before searching through your property. Medical records should be treated no differently.'"); Alissa J. Rubin, *Proposal on Privacy in Reverse*, L.A. TIMES, Apr. 21, 1999 ("'I had high hopes for this legislation when they started holding hearings on it last year,' said Denise Nagel, a physician and executive director of the National Coalition for Patient Rights, which is based in Lexington, Mass. 'So I was really surprised they came out pre-empting state law. ... States are just getting around to writing medical confidentiality law. ... You could drive a Mack truck through the holes in the bill.'")

[161] *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 Tex. L. Rev. 1, (November 1997) at 9 (arguing that Posner's argument that "if the lists are generally worth more to the purchasers than being shielded from possible unwanted solicitation is

the Act could enable widespread information piracy, of just the sort that even the music industry—with all its sophistication, statutory rights backing, and political power—feared in the absence of technical protection schemes. It is simply too easy for someone near a health information system to be *able* to abuse its contents, even if she is not *free* to do so. This may be clearer if we again frame the current Act and corresponding privacy regulations through the lens of copyright enforcement: it is as if Congress had actively promoted—nay, mandated—the development and use of the highly efficient and non-rights-architectured MP3 compression standards for digital music, leaving the formulation of protection from any abuse to a government agency which would prescribe general regulations lacking any private right of action.

Now imagine for a moment the patient control possible for these same three rights in a world where privacy advocates have succeeded in creating a trusted system that provides the patient with as much lopsided control over her medical records as the music industry's privication architecture seeks to provide for its intellectual property. Built on an ability to discriminate on the basis of consumer characteristics and on nuance on the provision of desired information to consumers with different kinds of interests in the data, the architecture could effect control not readily possible—not even administratively so—without it:

Suppose a patient could "log in" at any time to the databank of her one-stop HMO.[162] She could do so through her own personal computer over a secure

---

worht to the susscribers, we should assign the property right to the magazine; and the law does this" is preposterous, and that getting consent is worth the transaction costs).

[162] *See, e.g.,* Lawrence Gostin, *THE DATABASES, Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations*, ANNALS OF INTERNAL MEDICINE, Oct. 15 1997,

connection on the Internet, or through a terminal provided for this purpose at a library or health care provider. With a few mouse clicks she could view her own records as readily as a physician seeking access to them through similar computer-mediated means. She could view an audit log revealing who has seen her records and when, perhaps setting permissions as to whom among various categories of potential viewers—or even whom among specific people—is authorized to look at which pieces of information. She might, for example, want to exclude her notes from psychotherapy from easy access by anyone but her therapist, even if her therapist and primary care physician are employed by the same institution. She might want to allow those to whom she gives permission a chance to see the data but not save it—so an outside physician could look at her records but not print them or save a copy into another databank. The emergency room attending physician may be able to view an incoming patient's records for the duration of her visit to the emergency room, and lose access thereafter. This makes it possible for the record holder meaningfully to change her mind about certain disclosures to which she had previously agreed: she might allow baby products companies to know that she was recently in the clinic for an ultrasound related to a pregnancy so that they could identify her for the purposes of sending her coupons, but then revoke permission to include her name on targeted mailing

---

at 683-690 (describing a near-future medical information infrastructure in which patients, doctors, and health care organizations will be able to access conveniently patient information from centralized databases); Heather Green & Linda Himelstein, *A Cyber Revolt in Health Care* BUSINESS WEEK, Oct. 19, 1998, at 154 ("Longer term, the hope is the Web will go far beyond serving up medical data and will finally link together physicians, patients, and insurers like a massive electronic nervous system.").

lists should something go wrong with the pregnancy.[163] She might choose to allow a local pharmacy to view a list of her recent prescriptions at no charge, for the purpose of offering her a better pricing package, while charging an over-the-counter drug company $100 to see a record of her vaccinations, pre-paid. She might even ask that her spouse be permitted to make such rights determinations in her absence, or that in no case will her rights be more expansive than the list recommended (and electronically made available) by a privacy watchdog group.[164]

Indeed, she might only agree to the use of her medical data for marketing purposes so long as there is a division between those who conceive of a promotional mailing (and know its criteria) and those who actually view the mailing labels and affix them to the promotional materials for mailing.[165] An extreme implementation of the system would even allow the patient simply to

[163] *See* William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 Fordham L. Rev. 951, 953-954 (1996) (describing two years during which a woman was "bombarded" with baby-product samples, calls from baby photographers, and baby birthday wishes accompanying solitications, despite her miscarriage and subsequent attempts to be removed from marketing lists); *See id*. at 954 n. 25 (describing hospital's sale of woman's unlisted address to marketers after she delivered her baby there).

[164] Such a proxy would be similar to PICS, the Platform for Internet Content Selection, by which Internet users can ask to have web sites screened out on the basis of judgments by "raters" whom they trust to substitute judgment. PICS home page, (visited Nov. 29, 1999) <http://www.w3.org/PICS/> ("The PICSTM specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy. The PICS platform is one on which other rating services and filtering software have been built.").

[165] The third party would, in turn, have no knowledge of the criteria used to select the names on the labels printed. This compartmentalization of knowledge was not itself sufficient for a consumer reporting agency with a targeted marketing division to avoid the proscriptions regarding treatment of certain kinds of personal information under the Fair Credit Reporting Act. *See* Trans Union v. FTC, 81 F.3d 228, 233 (D.C. Cir. 1996). But it suggests one means by which less personal information can be divulged short of an outright ban on targeted marketing.

delete her records, or extract them from the system and keep them in her personal custody.[166]

While this hypothetical might seem appealing to some privacy advocates, it represents a balancing of interests that ignores most interests of the consumers of medical data—politically implausible at least, and perhaps even simply bad policy. It permits the possibility that Scott McNealy could frighten a wave of patients into deleting all their medical data en masse,[167] or that a particularly compelling telemarketer could flimflam patients into accessing and retransmitting all their sensitive medical information.[168] However, no matter how unappealing, these potentialities attest to the true range of power of trusted systems architectures.

I do not here seek to build a case for one or another particular allocation of rights and constraints with regard to medical records. Rather, I wish to emphasize that a well-designed trusted system of rights to medical data could be both powerful and flexible. The actual policy choices underlying what rights

---

[166] *Cf.* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 Fed. Com. L.J. 195, 240 (1992) ("Information networks may be structured to provide only the minimal amount of personal information necessary to accomplish a particular task and to delete personal information as soon as it is no longer needed.")

[167] See note 71, supra. (Edward Baig)

[168] *See* Susan Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 San Diego L. Rev. 1153, 1161 (In 1996, LEXIS-NEXIS introduced P-TRAK, which provides up to three adresses, as well as aliases, maiden names, and birthdates for over 300 million people, including Social Security numbers (at the time of its introduction). There was considerable public uproar and discussion in the media and on Internet discussion groups.); Laurie J. Flynn, *Lexis-Nexis Flap Prompts Push for Privacy Rights*, N.Y. TIMES CYBERTIMES (Oct. 13, 1996) (visited Nov. 29, 1999); Bruce Mohl, *Trading Privacy for Convenience*, BOSTON GLOBE, November 1, 1995, at 19 (discussing the pros and cons of Star Market cards which give discounts but also track shopping habits to help target advertising). <http://www.nytimes.com/library/cyber/week/1013nexis.html>; Regan, at 49 (discussing the difficulties of obtaining useful polling data about people's privacy preferences); Karen McNally Bensing, *Con Artists Scam Victims Over the Phone*, PLAIN DEALER at 2J, Jan. 4, 1998 (describing prevalence of scams and use of medical data by scammers to better identify prey).

architecture to build—what powers to grant to the patient and what exceptions to insist upon in a trusted system containing her data—are as difficult as any other policy choices involving rights (or property) allocation. The process by which HHS would determine how much "trust" to include in its interoperable standards, and whom to assign each of the sticks within a bundle of constraints, would itself be political. Privacy advocates would have to strategize to focus on just which elements of medical privacy were most important, and which could be left open within a negotiation at which other interests—medical research, government, direct marketing—are also well represented at the table.

Indeed, to the extent that privacy is simply a dignity interest, rather than a more readily calculable remunerative interest like protection of copyright, it is all the harder for those who embrace it properly to calibrate pressure to vindicate the interest to its perceived degree of importance, whether arguing for overall legal protection or weighing whether to pursue an individual action. Thus, if government is stepping in to subsidize and ultimately mandate a system for interoperable medical records, one may wonder why it should be any easier for patients to see their preferences reflected in that system as "trust" when their privacy has not been incorporated into traditional federal privacy frameworks to begin with. Isn't the public choice problem the same whether one is trying to convince Congress to mandate strong privacy rights as legal rules or within software code? I reflect on this issue in section V and argue that code helps break the logjam.

V. Beyond the publisher: Privication to satisfy both producers and consumers of data

Privacy advocates will only be able to benefit from the power and flexibility of a well-designed trusted system if it is politically and economically possible to implement one. A trusted system to protect music is emerging from market actors; apparently a handful of record companies—and technology companies—can overcome a collective action problem and invest in an interoperable protection scheme of benefit to all. There is no such phenomenon yet taking place for medical records; the collective action problem among millions of patients may make market-based development of a comprehensive medical trusted system quite difficult, just as it has been difficult for the market actors of hospitals, HMOs, and insurance companies to generate even an *un*trusted interoperable medical records system clearly of benefit to all.

Rather than being able to generate protection themselves, then, those who wish to protect medical privacy will be nearly as dependent on government intervention as they would be if they sought a legal rights-based solution. Yet their energy may still be better spent on the creation of a trusted system for medical records than on a new rule-and-sanction regime, because it will benefit them more than law and, done well, threaten competing interests less. The analysis of privication architectures in Part III suggests that it may yet be politically feasible, even desirable, for all those with a stake in rights to medical records—privacy advocates, medical researchers, and doctors alike—to create a trusted system that seeks to embed rights satisfactory to most interests.

First, so long as permissible and impermissible information practices can be defined in a way satisfactory to most interests—to be sure, a daunting challenge—consumers of medical data might well prefer an architecture where it is, as a technical matter, difficult to stray from authorized uses. The implementation of the trusted system could then be a safe harbor defense against a class action suit, agency enforcement proceeding, or other litigation-dependent remedy.

Second, privication architectures might help meet the daunting challenge of defining fair information practices, since the increased granularity of rights afforded by a technological system makes room for entirely new rights constructs. The expression of rights through a trusted system may allow for "baby-splitting" among interests that is not feasible in more traditional regimes. For example, in place of the stalemate over who should "own" a record, a well-defined self-enforcing rights architecture could allow information sharing without having to ultimately resolve matters in as coarse a way as "owner" or "non-owner." A patient might wish the right to delete her record, while medical researchers would object to the non-random loss of possibly important medical data. The system could enable deletion for "most intents and purposes"; one could imagine a deleted record no longer appearing on a hospital computer display, and no longer being available for marketing purposes, while still being included in scans of records by medical researchers. Just as a musical trusted system might distinguish between students and businesspeople—to enable price discrimination by the publisher—a medical trusted system might distinguish

among identities of those seeking to use the system, and among the purposes for which the access is sought. Indeed, the easy unbundling of songs from an album in the music context could become the unbundling of some data elements from others in patient records. A patient could release maternity information for marketing purposes while withholding HIV status; the government could still access the entire record (with process) for subpoena purposes if the entire record were deemed relevant, but otherwise it too, could get only the information needed for a particular purpose, such as payment information for fraud reduction efforts. For audit rights, a patient might be able to see everything in her record except that which is explicitly marked to be held back by an authorized doctor. Then, at least, she would have a sense of what she did not know and why, and her access to some parts of her record would not be held hostage to other parts deemed, for some important reason, off-limits even to her. All this could be done with a minimum of administrative burden on the database custodians.

The granularity of rights available within trusted systems also suggests that we need not choose between creating horizontally-integrated records (all records across a given institution) and vertically-integrated ones (all records pertaining to a given individual, wherever those records may be). Granting a patient seamless access to her records among all covered institutions means that getting a second opinion from an outside doctor—or transferring to another health care provider entirely—can be accomplished without the barriers of paperwork and delay endemic to patient access to current automated systems such as the MIB.[169]

[169] See Massachusetts Medical Information Bureau, note 107, supra.

This can promote competition without depriving institutions of the horizontal access to records deemed necessary to utilization review or other purposes.

Allowing granular "dynamic consent" for medical data could see patients electing to accept offers of all kinds for releasing their information, creating market efficiencies for the sale of vertically-integrated patient information where before there was primarily only the release of horizontally-integrated data by health care institutions. The system might even be constructed to allow patients to set preferences for access to some of their personal data, but discourage the creation of a market by denying them the ability to sell other data. Patients could thus be restricted from handing over highly sensitive information for a pittance without realizing the implications of the transfer, while still able to control other information. As various databases begin to converge—imagine the use a doctor could make of data on everything from one's genome to one's supermarket purchases, already recorded in many instances, to help design a healthy diet or correlate diet with a given disorder—an ability to efficiently set sophisticated gates around data elements could be critical. At the very least, a granular trusted system allows for those on the margins who care dearly about personal privacy to limit circulation of records, without requiring a similar default policy that binds all other patients.

Third, privacy advocates may learn from the music industry's structure rather than its technology: the use of aggregation of preferences may be applied to the problem of ill-informed (or simply disinterested) patients being asked to specify a battery of preferences about the disposition of their sensitive medical data.

ASCAP and RIAA are instruments of aggregation of preferences; to clear rights to a covered song one consults with ASCAP without having to reach the original author or performer. One could imagine an initial form presented to an incoming patient with some notice of the availability of a system through which to view records and exercise certain rights with respect to them. The form could ask a few coarse, basic questions, the answers to which would help fill in the initial patient-set constraints of the elaborated trusted system; it could also offer descriptions of three or four organizations whose preferences the patient could initially adopt as her own. Thus one could check a box, say, for the American Medical Association, the Electronic Privacy Information Center, or the AARP—importing preferences in one step that could be revisited at the patient's leisure later.[170]

Finally, trusted systems' Newtonian inertia of rights enforcement will help privacy interests over the long term given their weak political representation and power—once the system is in place, government cooperation is not nearly as important as it might be to traditional rights enforcement. The recent expansive history of federal copyright protection may well cause us to underappreciate this point, since the music industry has enjoyed an ongoing application of government protection and pressure to vindicate its rights before beginning to turn to trusted systems. Federal privacy protection, on the other hand, has more resembled the booth at the county fair where one attempts to swing a hammer so hard as to ring a bell overhead: it happens rarely, and the resonance fades not long after the deed is done. It does happen from time to time, however, and if

[170] See PICS supra note 193.

the pressure that brought about Federal privacy protection for video rental and drivers license records can be brought to bear for medical records in one concentrated swoop as the Department of Health and Human Services maps out privacy protection regimes through its rulemaking, the trusted system might be established and then resonate much longer thanks to its momentum.[171] Indeed, Congress might find it politically more difficult to undermine a privacy regime—to affirmatively strip privacy rights accorded by HHS—than to simply fail to pass legislation establishing the rights in the first instance. The physics of trusted systems are thus well suited to a Congress that only rarely allows a bite of privacy's legislative apple.

In a political environment marked by persistent stalemate, the conception of a privication architecture for medical records could encourage new compromise among formerly competing interests, and ultimately more privacy protection with a minimum of social cost.

VI. Conclusion

No practical combination of law and technology will be a panacea for the deep problem of control over information. Pinpointing the rights to be protected and the exceptions to apply is an ongoing exercise in civic discourse. The ability to elaborate those rights in detailed, self-executing ways could remove some

[171] Privacy advocates would presumably seek a "digital millennium privacy act" which would criminalize the cracking of a trusted architecture for sensitive personal data. However, this may not prove as critical to the success of the system as the DMCA is thought to be for copyright,

"give" in a system that also counts on norm and dynamic interpretation—respect for law, and for its substantive aims by those subject to it, and respect for the distinct circumstances of each case by courts enforcing it—to arrive at a just status quo.[172] In the case of privacy, only some of the matters of current pressing concern—for example, the routine use of personal information for marketing, employment, or insurance purposes—are satisfied by a trusted privication regime. Embarrassing personal details can be publicized as soon as an indiscreet (if authorized) viewer of personal data chooses to gossip, no matter how difficult it is for viewer to print the data or regain access to it later. However, despite its shortcomings, a trusted privication architecture for medical data offers a kind and degree of protection that law alone cannot easily emulate.

The Era of Promiscuous Publication is upon us, and for publishers of intellectual property the quite different Era of Trusted Privication is about to enter on its heels. A rare and fleeting chance for the latter era to come about for medical privacy in the United States is now within grasp. A system is already under construction specifically to leverage the fruits of the information age—quick processors, immense data storage, ubiquitous networks—into a drastic lowering of the costs of sharing personal medical data. The question is how much trust it will have—and who will be thought of as its "customers."[173] The government has already taken on the ambitious task of shaping a comprehensive set of standards

---

since the "elephant" consumers of medical data may count among them fewer rogues than the individual "gnats" who consume intellectual property.

[172] *Cf*. Meir Dan-Cohen, *Decision Rules And Conduct Rules: On Acoustic Separation In Criminal Law*, 97 Harv. L. Rev. 625 (1984) (defining acoustic separation as the intentional separation judges and legislators make between the law as stated and the law as applied in specific cases).

[173] See note 90, supra (TCPA) and accompanying text, supra.

for medical records interchange,[174] and private efforts are also under way to develop such systems.[175]

If the moment is not grasped now to develop and standardize privication architectures, the *un*trusted system for medical records now under development will have a momentum all its own. As the power of technology is harnessed to move us from a Gutenberg status quo of personal information sharing towards a more promiscuous one, we must consider means to impose agreed-upon limits that are grounded in that technology.

[174] See note 169, supra (Public Law, 1996 Act).

[175] *See* Patient-Centered Access to Secure Systems Online (PCASSO), *Provider's User Guide*, 1999 (visited Nov. 28, 1999) <http://medicine.ucsd.edu/pcasso/userguide.html> (offering secure viewing of confidential medical records on the Internet); Healtheon (visited Nov. 28, 1999) <http://www.healtheon.com/tech/index.html> (offering secure health care on the Internet); Stefik, The Internet Edge, 208. This particular "patient-centered" system builds in both power and limit to patient access: the patient can view audit trails, but a physician's access cannot be limited by the patient, and the doctor may selectively screen substantive data from the patient's view. The patient cannot delete or, it appears, copy any records in the system.