NYSBA WINTER 2000 | VOLUME 9 | NO. 3

Bright Ideas

A publication of the Intellectual Property Law Section
of the New York State Bar Association

Message from the Chair

We are back from the best Lake George conference ever, filled with engaging, practical, and provocative discussions about the Internet and intellectual property. We also enjoyed a spectacular fall weekend with leaves at near peak. Many thanks to Rick Ravin, Michael Carlinsky, Marc Lieberstein, and our outstanding speakers and participants for making it a perfect way to get together, explore ideas, and have some fun. We hope to see you at the conference next year. We have already booked the dates—October 11-14, 2001.

One of the high points of our fall event is the announcement of the winners of our student writing contest, sponsored by Thomson & Thomson. Over the years the contest, student participation, and the prizes have grown. This year we awarded a prize of $2000 to Michael Kasdan of New York University School of Law for his article on eCommerce business method patents after *State Street*; $1000 to David Johnstone of SUNY Buffalo Law School for his paper on the unauthorized use of MP3 on the Internet; and $500 to Donna Furey of St. John's University School of Law for her paper on WIPO protection of audio-visual performances. Darryll Towsley of Albany Law School (and the Section's photographer) won honorable mention for his paper on the intellectual property implications of the Microsoft antitrust case. Congratulations on such fine submissions. Two of the winning papers are published in this issue of *Bright Ideas*. And many thanks to Thomson & Thomson and our panel of judges. We hope that if you are or know a student member of the Section, you will pass the word about the competition. Please contact me, vacundiff@phjw.com, Walter Bayer, walter.bayer@corporate.ge.com, or Jeff Cahn, jcahn@sillscummis.com, for more information about the competition.

As the leaves turn we are looking ahead to our next big event, the Annual Meeting of the Section, to be held at the New York City Marriott Marquis on

Inside

January 23, 2001. We will be concentrating on "New Developments in Intellectual Property Law: A Look at Law, Policy, and Practice." We will be hearing from representatives of the Patent and Trademark Office, the Copyright Office, the courts, practitioners, and business people who have developed and exploited intellectual property and who have some ideas on how the law can help serve their business interests. We look forward to seeing you there.

We want to work hard to build a community within the Section that transcends our two big events. To that end, several of our committees have regular lunch meetings to discuss new developments in their substantive areas. We will post a calendar of events on our Web site. We hope you'll attend in person or by conference call. If you'd like to host or participate in these smaller meetings, please let us know. We'd also like to get working groups going across the state, including an in-house counsel roundtable at which we can share and learn from practical tips that help on a day-to-day basis. Finally, we look forward to submissions of forms, briefs, and other interesting intellectual property items for our Web site.

We look forward to getting to know you and working together to learn and develop intellectual property law.

Victoria A. Cundiff

Thank You

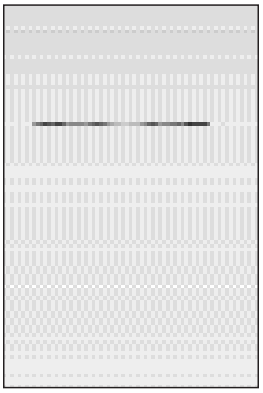
The Intellectual Property Law Section extends its gratitude to the following firms, as well as THOMSON & THOMSON, INC., for their significant sponsorship over the past year:

- Pennie & Edmonds LLP
- Cowan Liebowitz & Latman, PC
- Jacobs, DeBrauwere & Dehn
- Kirkpatrick & Lockhart
- Orrick Herrington & Sutcliffe, LLP
- Ostrolenk, Faber, Gerb & Soffen, LLP
- Paul, Hastings, Janofsky & Walker LLP
- Sills, Cummis, Radin, Tischman, Epstein & Gross, PA
- White & Case LLP
- THOMSON & THOMSON, INC.
- Cybersafe

The Pirates Are Always With Us: What Can and Cannot Be Done About the Unauthorized Use of MP3 on the Internet

By David R. Johnstone

I. Introduction



As a potential medium for unauthorized recordings, MP3 is not an empty threat to music copyright interests. This "open source"[1] compression standard[2] (or "codec")[3] of choice for music files on the Internet, on the eve of the millennium, has rung disc(h)ord across the international recording industry, and its implications have confused copyright lawyers and scholars. MP3 is a controversial format because it contains no built-in copyright-protection scheme of its own, and it allows effortless duplication and sharing. It is thus a pirate's dream and a copyright holder's nightmare.[4]

Due to MP3's digital nature, successive copying does not compromise fidelity. In this respect, it is superior to conventional magnetic tape, which has a propensity for "generation loss" with each successive copy of a copy. This means that an nth-generation edition of an MP3 file could sound just as clear and desirable as the initial source copy. Accordingly, the widespread use of MP3 poses a threat to the copyright holder's right of distribution because unauthorized, homemade copies could significantly replace the public appeal of sonically indistinguishable copyrighted merchandise.[5] In an age when proprietary material can be beamed all over creation with a mouse click, the number of copies in circulation can become frightfully disproportionate to collectible royalties.

MP3 allows a musician to spread his or her music like pollen, but at the same time it allows countless others to replicate it like bacteria. (The metaphor depends on the motives of the party sending the electronic cargo.) As MP3 files are, to date, easily exchangeable, innumerable copyright holders will go unpaid for an incalculable number of consumers' copies. All too often, the copyright holder is not a part of the transaction or equation in online music distribution—yet another example of a rising tide that *does not* lift all boats. The grand challenge at hand is to sink the ones that sail under pirate flags.

Normally, a music copyright holder enjoys the right of control over distribution of copies only at the time of "first sale,"[6] and thus can neither stop nor claim payment from the subsequent trade of used copies. With the MP3 format, however, the first sale of a single copy, whether as a CD or an official downloaded version, might be the only commercial dealing to precede an unlimited number of consumers' acquisitions of copies of that work. In this respect, MP3 duplication and distribution can support and promote a free-for-all—a boon to anyone except the rightful collector of royalties (or, for that matter, retailers and other interests associated with the recording industry). To make another party's copyrighted recording openly available to the masses is, effectively, to hijack the master copy and to establish one's own fly-by-night CD-pressing plant. There is a far cry between rightfully turning over one's own used copy of a CD upon exchange for something else, on the one hand (thus terminating ownership in that individual copy), and using the binary stream on that very CD to blaze an unlimited distribution channel online, on the other, whether or not for material gain. The former is called trading; the latter is called piracy.

The first-sale implications of MP3 would have the same complexion as any other recording format if a consumer were simply to sell (or even give away) his or her very copy of a music file, which happens in the not uncommon trade of used CDs. However, with the meteoric rise of online swap meets like Napster,[7] the tendency today is to give or trade imprints of MP3s on and on, around and around. MP3 exchange perverts the traditional concept of alienation because possession does not shift at acquisition—only a cloned file, not the original, passes.[8] The transmission process is analogous to the spread of news, or of communicable diseases, as distinguished from the quid pro quo model of trading tangible items, such as baseball cards. MP3 files, therefore, are potentially gifts that keep on giving, but from a copyright owner's perspective they can serve as instruments of deprivation when would-have-been consumers acquire them by dodging the marketplace.

The scourge of MP3 piracy in particular is already entrenched throughout the United States and much of the developed world—particularly among computer-equipped youth. It has soared in the past year, particularly with the popularity of Napster.[9] Although criminal sanctions and civil causes of action are provided for in the United States and elsewhere (in addition to recent and anticipated technical safeguards by various indus-

tries),[10] MP3-based music piracy will remain a fact of life for music copyright holders for the foreseeable future. Most countries do not currently have antipiracy laws drafted expressly for the cyberspace context.

Much of the pirate traffic in MP3 is done non-commercially, in a Robin Hood-like spirit. To an unprecedented degree, private individuals—often with little or no understanding or appreciation of copyright law—are making professional musicians' intellectual property music available to anyone with access to an Internet terminal, like so many localized looters in a global riot. Due to the clandestine nature of piracy in general, and to the private and unmonitored nature of e-mail traffic,[11] the true extent of illicit MP3 activity is simply inestimable. What began as a closely practiced hobby eventually graduated to the status of a trend, and it is now a ubiquitous craze.[12]

Illegal recordings, in one format or another, have been a thorn in the side of the international recording industry for over thirty years,[13] but widespread, cutting-edge technology now vastly increases the danger to the proper collection of payments (be they royalties or licensing fees) that are legitimately owing for the distribution and use of recordings.[14] The most formidable foes of online intellectual property today are not legislators, litigants, lobbyists, or Luddites, but loyal-opposition pirates and their twin brothers, hackers,[15] on the supply side, and the freeloading consumer,[16] who wants something for nothing, on the demand side. Copyright holders everywhere are now more vulnerable than ever to misappropriation by non-paying users everywhere, to the extent that pirates give freebie seekers such an opportunity. Aggregated lost revenues can be very difficult to assess.

Ever since the Industrial Revolution,[17] technological developments have consistently maintained a handy timing lead over applicable law. Such is the dual action-reaction relationship between scientific progress and governmental regulation. The gap is ever-widening in the Internet Age, as new applications and uses present themselves and mushroom with increasing frequency. International treaties; existing domestic statutes; new or amended legislation; criminal prosecution; and civil litigation, however, will not suffice to contain or curtail online piracy of music or, for that matter, of other information media. These measures have been consistently reactive, not proactive. They tend to be much too little, much too late.

At present, copyright holders and public authorities have access to several juridical weapons with which to combat electronic piracy, but they will need to learn to use several of them in tandem in order to have any impact upon the extent of electronic theft of music. The entire recording industry will have to embrace the new regime of e-commerce and supplement its twentieth-century, brick-and-mortar business models if it is to beat the MP3 pirates at their own game by retaining freeloaders as retail customers. Once the necessary security measures are perfected and fully in place—including legal, cross-industrial, and international schemes—record companies should adapt by adopting MP3 and its progeny as salable formats. (To do so will require a secure micropayment system that will accurately tally and remit royalties.) Those record companies that implement a direct-delivery, e-commerce model will be far more able to capitalize on a convenient and cost-effective market—particularly for single tracks, which declined with the obsolescence of the seven-inch, 45-rpm vinyl record.

An effective antipiracy climate in cyberspace has been, and will continue to be, slow to establish itself. In the meantime, copyright holders will remain sitting ducks. Their work and/or property will continue to be available for the taking, in the virtual public square. Their copyrights will continue to be suffocated by blasé attitudes about rich rock stars and faceless corporations that do not seem, on the surface, to be vulnerable to isolated incidents of limited copying. At the time of writing, online piracy via one channel or another is just too easy, and for many opportunists it is just too enjoyable. In the minds of many consumers with limited music budgets (particularly youth), it also beats paying $17.00 or more for a whole CD on which there may be only a few appealing tracks.[18]

Eventually, MP3 piracy may well be driven somewhat underground in the wake of stepped-up enforcement—as has happened to the unauthorized trade in CDs, VHS cassettes, and computer software, for example[19]—but under the current aggregate of countervailing factors, it will endure as popular sport unless or until a more copy-proof technology supplants MP3 as the favored medium of the day.[20] In the meantime, record companies should hasten their efforts to seize the hungry market and make online distribution—also known as "digital phonorecord delivery"[21]—just as appealing and available to the public as are the burgeoning non-market channels with which they are, de facto, competing.

Never before has high-quality, amateur copying of digital recordings been so easy. Freely downloadable CD "rippers"[22] and "encoders,"[23] and low-cost "burners,"[24] are now available. More and more computer users are acquiring the necessary means to distribute, receive, and preserve exact copies of near-perfect sound recordings. With the right tools in hand, anyone can traffic in copyrighted material, and with unprecedented expediency. Hardware that can be used for the unauthorized dissemination of copyrighted material is already amply widespread among the mainstream com-

puting public—at home, at work, and at school—and will become only more commonplace in the future.[25]

II. MP3 Up Close

MP3[26] was developed in 1987—light years ago in Internet terms—at the Fraunhofer Institute Integrierte Schaltungen (IIS),[27] a German applied-research center, as a means to compress digital signals. Its unforeseen popularity as a music medium in the cyberspace community did not sprout until about 1997, however. The software technology itself is not illegal, although it is frequently used for nefarious purposes.

MP3 cuts the number of bits in a digital music signal to between one-tenth and one-twelfth of the original size.[28] It operates on a "psychoacoustic" principle to jettison encoded data for all but the very sound that the human ear can perceive.[29] No longer must whole tracks be prohibitively large for the average home computer system, as had been the case prior to widespread compression standards. The MP3 format can pare the average 60-megabyte (MB) track down to about 5 MB, with a single megabyte being able to hold about a minute's worth of converted stereo music signal.[30] Downloading a complete MP3 track at 56.6 kilobits per second (kbps) takes only a matter of minutes.[31]

To make an MP3 file of a track from a CD, a user first "rips" (figuratively) the binary stream of a track from its source medium.[32] To date, commercial CDs have not been factory-encoded with security features to prevent ripping, or uploading after ripping. The signal is then converted to MP3 format by stripping out extraneous data so that only the necessary minimum is retained. Once this encoding step is completed, a user can upload the MP3 file to the Internet by posting it on a Web site or in any of the unregulated, special-interest newsgroups in the Usenet family,[33] or he or she can attach it to a private e-mail message to friends, family, coworkers, classmates, or anonymous, global contacts made via a service like Napster or in a "chat room."[34] After uploading, the user is fully able to retain a copy of the file (unless, or course, he or she deletes it or it becomes corrupted). The public conduction process can occur over and over again, with unlimited freeloaders on unlimited receiving ends, which can be converted to unlimited bartering opportunities. Digital music thus becomes a renewable resource like no other.

MP3 files require special playback software, aptly called a "player," to run on the desktop. At the time of writing, the most popular MP3 player software for use with Windows is called Winamp.[35] The Macintosh player of choice is called Macast.[36] Several MP3-specific search engines[37] have emerged, most notably http://mp3.lycos.com and http://www.audiofind.com. They do not distinguish rogue sites from the authorized locales (such as eMusic, formerly known as GoodNoise) that pay statutory royalties[38] in accordance with the "Digital Phonorecords Distribution" (DPD) license granted by a publishers' clearinghouse like the Harry Fox Agency (HFA).[39] eMusic, for example, distributes MP3 files online on behalf of independent (or "indie") label Rykodisc and "submit[s] regular reports to HFA, account[s] for each song purchased, and pay[s] the appropriate statutory payments to HFA for distribution to copyright owners."[40]

III. The (Current) Popular Appeal of MP3

Convenience and price account for most of MP3's mass attraction. The format allows the transmission of music files to be unusually time- and space-effective. Especially in contrast to the common but bulkier "wav" files,[41] the MP3 format provides an ideal, expedient way to obtain entire song files. One counterintuitive feature of the technology, however, is that its fidelity does not represent a leap forward. In fact, its sound is often described, at best, as "near-CD quality."[42] Many desktop PCs' small speakers, moreover, do not do wonders for recorded music, but millions of MP3 users have willingly turned their CPUs[43] into de facto stereos nonetheless, with the aid of headphones. A few have craftily rigged their soundcards to their component sound systems, and in late 1999 a company called X10.com rolled out a wireless gadget called "MP3 Anywhere," which sends the MP3 signal from the CPU to a plug-in unit in the headphone jack of a stereo receiver up to one hundred feet away.[44] Also in 1999, several manufacturers introduced in-dash, car-audio MP3 players.[45] MP3 has truly arrived.

From a consumer's standpoint, track-by-track downloadability also promotes flexibility where it has not existed before. In an online marketplace, the format allows an à la carte choice of titles to buy. Now, one can decline uninteresting tracks by an artist or group rather than having to pay bloated retail prices for a full CD that might well contain several "filler" tracks or "throw-aways."[46] In true roll-your-own style, one can also "burn" (i.e., mint) homemade CD-Rs[47] in any customized configuration one prefers, and can play them back in PCs' CD-ROM drives. College students, for example, can pursue this pastime in common computing centers or in the privacy of their own dorm rooms. Many schools now provide direct access to lightning-fast T1[48] or even T3[49] connections, which put respectable 56.6 kbps, copper-line modems to shame.

Many recording artists are also embracing MP3 as an alternative delivery medium.[50] Some of those who have adopted the format have been disenchanted with their own business dealings with record companies, and some are fledgling bands whose only viable option is to distribute their music online directly, to a listener base, absent a recording contract. Ironically, an ensem-

ble or artist who would circumvent the traditional label route would thus forgo valuable promotional backing, so this marketing approach may prove to be of limited impact among all but established or quickly rising acts.

What ultimately brought MP3 out of relative obscurity and into the public consciousness and controversy as much as any other forces were the advent of the "Rio," a portable, Walkman-like MP3 player,[51] and the recording industry's recent, but unsuccessful, attempt to have it banned from the market. In the recent decision in *Recording Indus. Ass'n of America v. Diamond Multimedia Sys., Inc.*,[52] the Ninth Circuit frustrated record companies' antipiracy efforts and confused many who thought that they had known (intuitively, at least) what a "recording device" was. The court's decision gave the green light to the mass production and marketing of portable, MP3-playing devices, and in turn shocked and scared the recording industry into facing the Internet Age.

IV. Applicable Statutes

1. Audio Home Recording Act (AHRA)

The Ninth Circuit's rationale in the unanimous *Diamond Multimedia* decision was based on a curious, often counterintuitive, but unanimous, interpretation of the Audio Home Recording Act (AHRA).[53] This 1992 statute, which added a new Chapter 10 to Title 17 of the U.S. Code, had been drafted in anticipation of the rise of digital audio tape (DAT) devices. It permits consumers to reproduce their own copy of a sound recording, for non-commercial purposes,[54] and requires digital audio recording devices to contain a "Serial Copying Management System" (SCMS)[55] to control the replication of digital (and thus exact) copies of a recording.[56] It also requires their manufacturers to pay minor statutory royalties to record companies in order to offset potential economic losses resulting from home taping.[57]

Diamond[58] had neither implemented an SCMS scheme nor paid the AHRA's statutory royalties on units sold. The RIAA had sued the manufacturer of the Rio, which can play any MP3 file, whether legitimately downloaded or not, or whether "space-shifted"[59] from a legitimately bought CD, or not. The suit alleged that the Rio is a digital audio recording device, subject to the provisions of the AHRA.[60] Diamond countered that AHRA did not apply to computers or to peripheral devices and that the Rio was just a playback device—not a recorder—and thus exempt. The manufacturer won, and now Web-using music consumers have an approved, accessible new hardware dimension to their hobby. The court held that the Rio is not a "digital audio recording device" within the terms of the pre-MP3-era statute. Although the product clearly records digital music (through a cable running from a port in the CPU), the court distinguished it from technology like the now-obscure DAT recorder. It noted that the Rio cannot make subsequent copies, and does not record directly, but rather takes on data from an intermediate, multi-purpose hard drive.[61]

Computers and storage media like CD-Rs do not fall within the purview of the AHRA, even though they are fully capable of holding, providing, or receiving unauthorized recordings, such as infringing MP3 files. A hard drive is not exclusively an audio recording device, so computers need not comply with the AHRA's SCMS requirement. The distinction lies not in the individual consumer's primary, or even exclusive, use of an individual appliance, but in the primary purpose for which a product is designed and sold. Consequently, the manufacturers of multi-purpose devices that are equally capable of producing an illicit digital recording neither pay the statutory royalties nor include SCMS measures. The AHRA is limited in its ability to stop or slow MP3 piracy, as the Rio decision confirms, so copyright holders will have to look to other statutes for more effective protection from pirates.

2. Digital Millennium Copyright Act (DMCA)

In late 1998, President Clinton signed the Digital Millennium Copyright Act[62] into law. The statute implements the terms of two as-yet unratified treaties of the World Intellectual Property Organization (WIPO), an arm of the United Nations: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, which were finalized in Geneva at the end of 1996. These two treaties, which require signatory nations to protect rights in each other's copyrighted works, are intended to revise the current Berne Convention for the Protection of Literary and Artistic Works.

The DMCA outlaws the circumvention of "technological protection measures."[63] Such actions include the defeating of user-specific lock-and-key encryption schemes. This provision is especially relevant to MP3 piracy because of recent cross-industrial initiatives to encode copyrighted recordings with "digital watermarks," which could prevent the playback of illegitimate copies.[64]

The DMCA exempts Internet Service Providers (ISPs) from liability for unauthorized, copyrighted material contained in their users' transmissions or on Web sites that sit on the providers' servers, as long as the providers did not know of the presence of infringing material in their midst; did not derive any financial benefit from the use of such material; and acted "expeditiously to remove" or block such material upon formal notification (as by the RIAA, for example) of its presence on their systems.[65] Receiving revenue from a Web site's banner ads could constitute financial benefit associated with the activity.[66]

An ISP must name an agent to receive notice of any infringing material.[67] The U.S. Copyright Office's Web site[68] maintains a list of ISPs' infringement-notice agents. Providers are not naturally inclined to police perpetually every stretch of bandwidth[69] on their servers at all times, so the "notice and takedown" provisions of the DMCA depend largely on the diligence of watchdogs who may or may not happen upon the infringing material immediately.[70] Given the amount of MP3 files in cyberspace today, a copyright holder could face a considerable time investment in order to seek and silence unauthorized downloadable editions.

The DMCA will strengthen international mutual protection of copyrighted materials, but it is beyond the ability of Congress to ratify the WIPO treaties: They will not be binding until thirty nations have signed them. In the meantime, the United States remains a signatory to the Berne Convention for the Protection of Literary and Artistic Works, which copyright scholar Paul Goldstein describes as requiring "essentially an act of faith, faith that the other member countries will extend copyright protection to the works of foreigners on at least the minimum terms in the treaty."[71] One of the other problems with the Berne Convention, as Goldstein points out, is that there are no enforcement procedures associated with it.[72] Of course, the sticky and unresolved issue of jurisdiction in cyberspace makes harmonization of international laws all the more important, yet elusive.

The DMCA's immunity provisions thus will provide an incentive for ISPs to intervene when necessary, and they will make it worth while for ISPs to be vigilant in responding to alerts of violations in their own backyards. The security-circumvention provisions will also deter some of the less tenacious (and less brave) hackers from crashing toward protected material that they do not have permission to access, but we should be cautiously pessimistic here because hackers have always been notorious for persisting in efforts to raise the bar of computer mischief.[73] To date, there have been no appellate decisions interpreting the DMCA. Future cases will likely include litigation against ISPs who do not remove unauthorized MP3 files "expeditiously" enough.

3. No Electronic Theft (NET) Act

The cause of antipiracy gained a more potent criminal statute in December of 1997 with the signing of the No Electronic Theft (NET) Act,[74] which had passed unanimously in each house.[75] Willful infringement for "commercial advantage" or "private financial gain" or, during any 180-day period, reproduction or distribution of one or more copies or phonorecords of one or more copyrighted works with a total retail value of over $1,000, can now result in a six-figure fine and a sentence of up to three years in prison.[76] Penalties increase for repeated offenses and in proportion to the extent of infringement.

The NET Act finally closed the pernicious "LaMacchia loophole," which had allowed persons to escape criminal liability for posting proprietary materials online without authorization if they did not receive or derive any commercial benefit from their actions. The statute is a legislative response to a federal case involving a former MIT student, David LaMacchia, who ran a bulletin board system[77] called Cynosure, which encouraged members to upload software programs to it. LaMacchia would then move the proprietary material to another location, from which users with a password could access it and download it at no cost.[78] LaMacchia was arrested for copyright infringement, but ultimately the district court acquitted him because he never had realized any financial or material gain, and so his actions had not been, technically, illegal under U.S. copyright law. Nevertheless, many copyright holders' valuable material was exposed in the public forum (i.e., cyberspace) for unlimited, unauthorized, free copying. Following the disappointing outcome in court, the software industry lobbied heavily for legislation to close the loophole.

The NET Act defines "financial gain" to include "receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works."[79] Not a cent need change hands in order for liability to attach, and thus the criminal statute brings a substantial number of amateur MP3 users within its crosshairs, particularly those who traffic in high volumes of material. A victimized copyright holder may submit a "victim-impact statement" to describe and quantify his injuries,[80] but giving meaningful information can be a tricky proposition: In any given case, there might not be any preserved record, such as a visitor counter on the infringing Web site, to use as evidence of the extent of freeloading. Furthermore, the statute is not entirely clear as to whether each "hit" by a freeloader (which may or may not even result in a successful, complete download of one or more pirated files) constitutes a separate count of infringing distribution. That is a matter the courts will have to decide in the inevitable future cases.

In November 1999, the U.S. District Court for the District of Oregon meted out the first sentence under the newly passed NET Act, in a case that partly involved MP3 piracy. Jeffrey Gerard Levy, an undergraduate at the University of Oregon, received two years of conditional probation[81] for criminal copyright infringement under 17 U.S.C. § 506(a)(2) and 18 U.S.C. § 2319(c)(1), having pled guilty three months earlier to charges that he had posted music files, computer software, entertainment software, and digital movies on his

Web site—all on the school's server.[82] University officials alerted legal authorities after they noticed and investigated an unusually high level of bandwidth traffic in connection with Levy's Web site.[83] The FBI and Oregon State Police obtained a warrant to search the student's apartment, and then seized his computer equipment. Levy's Web site was found to contain copyrighted software, music files, and clips from feature films, but due to the novelty of the case and a shortage of resources, the U.S. Attorney's office did not conduct a full forensic test on Levy's machine, so they were unable to discover the identities of any of his piracy associates or correspondents.[84]

For the volume of piracy alleged, Levy could have received a three-year prison term and a fine of up to $250,000, but the court was unable to determine a reliable figure for the total value of the posted material in question. (Levy agreed that it was more than $5,000.)[85] Sentencing guidelines for criminal copyright infringement are based largely upon the total retail value of the material in question.

Although the NET Act makes criminal prosecution for MP3 piracy substantially easier, it cannot act as a panacea within today's Internet climate because there are too many convictable pirates (often acting correspondingly as freeloaders as well), and only finite public resources for enforcement. The federal government has a shiny new weapon in the NET Act, but it is massively outgunned by a nation full of rebellious and/or law-ignorant or -apathetic youth.[86] Some measure of justice will always be possible as a result of the NET Act, but it will represent a mere drop in the pirate-infested waters. The Levy case sends a message to MP3 users (if only they would hear it!) that the federal government is making the interdiction of Internet piracy one of its priorities. What remains to be seen, however, is whether the public cares enough to reform its proclivities, and the extent to which the federal government continues to crack down on private individuals. As with most facets of the judicially uncharted MP3-piracy controversy, only time will tell.

4. Recording Industry Responses

The recording industry continues to mobilize against MP3 piracy. The RIAA has tremendous financial resources and now focuses a considerable portion of its antipiracy budget on Internet-related offenses. In addition to its legal teams, it employs a staff of full-time Internet surfers who scour cyberspace for unauthorized music content.[87] Much of its challenge lies in finding the infringing host sites, and then in figuring out who operates them. The association also runs a whistleblower hotline program called "Badbeat," which receives and responds to reports of known and suspected music piracy.[88]

In 1999, the RIAA estimated that forty percent of illegal Web sites are located on college servers.[89] Tracking the files that are posted on these networks is easy enough to do from a remote location (that is, with a search engine or special tracking software), but it is another proposition altogether to police individual students' own hardware, where many illicit MP3 tracks are likely lurking.[90] Some schools take a decidedly hands-off approach to students' use of copyrighted material on common servers.[91]

The RIAA also has struck back at institution-based online music piracy with a program called Soundbyting,[92] by which it educates college administrators and students about the realities of piracy, including illegality and victims' available remedies. Over three hundred universities had joined the program as of late October 2000.[93] The RIAA reports a modest, but encouraging, ten percent drop in piracy on member schools' servers as a result.[94]

Many schools have taken a proactive stance on the issue. Carnegie-Mellon University, for example, undertook a random sweep of students' accounts located on the school's servers in November of 1999, in concert with RIAA's Soundbyting program.[95] The effort turned up a potato field of unauthorized MP3 files, and the school soon disciplined the staggering total of seventy-one students at once. (One of the hazards of this kind of sweep, however, is subsequent privacy-rights litigation.)[96] Their punishment seemed little more than a slap on the wrist: loss of (authorized) university network accounts for what little remained of the semester, and mandatory seminars in copyright law. The latter is generally a meaningless exercise for users who are aware of, yet incorrigibly irreverent toward, the gravity of unauthorized use, or who find a certain romanticism in the notion of contraband. At the time of writing, no criminal charges had been filed in connection with the raid. A similar search at the University of Florida found that 1,100 students (of 43,000) were pirating music on the school's servers, but a subsequent search, after processing the disciplinary cases of all of those students, turned up only seventy-three offending files.[97] Several dozen other cases at the same school have arisen from roommates blowing the whistle on each other.[98]

The International Federation of the Phonographic Industry (IFPI) has been mounting various global efforts as well. In March 1999, for example, the association pressed criminal charges against the FAST Search & Transfer ASA search engine, a Norway-based compiler of links to MP3 files on the Internet.[99] FAST had licensed its search engine and database to Lycos, another search-engine operator.[100] Most of the files to which it provided links were unauthorized.[101] The IFPI's French, Czech, Finnish, Swedish, Danish, and German offices

have similarly pressed criminal actions and have petitioned for injunctions against various Web site operators who propagated illegal MP3 materials. Since June 1998, over eighty letters have gone to operators of pirate Web sites in South Korea, with a shut-down success rate of about two-thirds.[102]

In November 1999, the IFPI announced another global antipiracy campaign. It will pursue two principal categories of targets: parties who upload unauthorized music, and the ISPs that host sites containing any such files.[103] This initiative will involve sending warnings and cease-and-desist letters, as well as filing civil actions against those who do not comply with demands to remove the unauthorized content. In the past year, the IFPI has filed civil suits against operators of Web sites in China, long a mecca of CD and software piracy.[104]

One of the key, but unsettled, issues in Internet law generally is that of jurisdiction. This is one reason why international treaties are so important. Fully equipped Web users can be situated just about anywhere, even in much of the developing world. At least where U.S. jurisdiction applies, the encoded music that traverses the globe in the form of MP3 files is unmistakably subject to U.S. copyright protection, although the more specific issue of venue may take some working out. The IFPI's international initiatives, of course, cannot function optimally without the continued cooperation and sympathies of police forces and courts worldwide, who might or might not (yet) consider digital music piracy to be an urgent threat to domestic economic interests.

In 1999, the Japanese Society for Rights of Authors, Composers, and Publishers (JASRAC) has embarked on an ambitious security plan, tentatively called "Dawn 2001," which aims to encode anti-copying, work-specific data into official, factory-made CDs.[105] The data in the binary signal would survive a compression process and allow the tracking of illegally distributed MP3 files made from these CDs.

Although Dawn 2001 is a clever idea, it is still far from fruition. It is the sort of effort the recording industry should have developed years ago. In the meantime, mountains of music remain unprotected. Alas, this kind of safety measure likely will not cover the full range of CDs under the group's authority because of preexisting unprotected CDs and the high volume of knockoff CD trafficking.

V. The Secure Digital Music Initiative (SDMI)

At the end of 1998, over 120 organizations and firms from various international electronics and music-related industries formed a consortium and embarked on an ambitious anti-piracy mission called the Secure Digital Music Initiative (SDMI).[106] SDMI has been mistakenly called a technology, but it is really an in-progress, cross-industrial forum for developing a "voluntary, open framework for playing, storing, and distributing digital music necessary to enable a new market to emerge."[107] SDMI's aim is to develop "an overall architecture for delivery of music in all forms,"[108] not just MP3. Most record companies have been wary of selling music via digital phonorecord delivery without an effective infrastructural antipiracy plan in place. Like any compromise that tries to be too many things to too many parties, however, SDMI alone will not be enough for copyright holders to gain a sustainable strategic advantage in the ultimately unwinnable war on MP3 piracy.[109] If SDMI ultimately succeeds in its efforts, it will be a key battle victory at a critical time, amidst a Wild West mentality that regards online copyright protection as an oxymoron, repugnant, or just an antiquated vestige of pre-digital times.

SDMI has developed with an eye toward two principal phases of implementation: Phase I, announced in June 1999, calls for agreement on SDMI's technical specifications and the platform in which portable MP3 players would operate.[110] These devices will play music files in all digital formats, whether protected by security technology or not. They are expected to be upgradeable to accommodate a still hazy Phase II security plan by some point in 2001, although device owners will not have to upgrade their units.[111] This lack of obligation is worrisome because if the listening public should choose not cooperate with SDMI's plans, the initiative will have little impact. (A survey of Phase I player owners, conducted just after the start of Phase II, would be an excellent way to gauge public receptivity to SDMI in general, and therefore would be a useful predictor of its success.) Neither Phase I nor Phase II will prevent users from ripping and uploading music, or from downloading any unauthorized music that will undoubtedly continue lurk in the more shaded crevices of the Internet.[112]

A special screening technology will be built into the next generation of portable players. It will scan the binary signal for a digital "watermark,"[113] which has been chosen but not yet implemented.[114] Accordingly, Phase II-compliant devices will reject pirated copies of post-SDMI-released content only.[115] Since the announcement of Phase I in August 1999, ARIS Technologies, Inc. has licensed its proprietary watermarking process, "ARIS-SDMI-1" (based on U.S. Patents 5,774,452; 5,828,325; and 5,940,135), to the SDMI-member manufacturers of portable devices like the Rio.[116] Artists and record companies can choose whether or not to encode their releases with the inaudible watermarks.

In the near term, SDMI will be of limited effect in preventing piracy, but eventually it could become the copyright-protection standard worldwide. It will have

to be much more carefully crafted. One looming hazard is that consumers who buy primarily used CDs might not even bother to upgrade their devices for Phase II because their collections will not contain the forthcoming digital-watermark security system. Perhaps the most major threat to SDMI, however, is a cracking of the code it will use. After the 1999 DVD code breach,[117] defeating the SDMI security measures (a violation of the Digital Millennium Copyright Act) could be the hacker community's next Holy Grail.[118]

VI. Conclusion

Members of the recording industry are starting to learn, particularly in light of the Napster phenomenon, that the consumer market likes MP3's convenience and demands digital phonorecord delivery.[119] When a secure MP3 retailing system is in place and/or a workable successor format emerges, the Big Five record companies will be in a position to embrace and promote the downloadable music movement. (After all, film studios were once very nervous about the potential ascendancy of the video cassette recorder in the home, but one of the results of their failure to repress that technology in court is that more than half of the film industry's revenues now derive from home video.)[120] These firms may even find it profitable to lease advertising space on their e-commerce Web sites. When they realize just how lucrative the new order is and will be, they will praise the Ninth Circuit's Rio decision for all that it is and will be worth to them in terms of consumer revenue, but only if they can provide an alternative that is no less appealing than copying copies of copies.

Estimates vary sharply as to the percentage of retailed music that will be distributed online, by which future year. Some experts forecast the numbers as high as 80 percent of commercially sold singles within five years.[121] Market research firm Forrester Research projects the total annual value of commercially downloaded music to top $1 billion by 2003.[122] Jupiter Communications, however, puts the figure at closer to $150 million by the same year.[123] Whichever is the more reliable figure would be even higher except for the inevitable piracy of the day, which will be difficult to quantify.

It will take some time to analyze the behavioral trends of a market within a whole new model and a whole new set of purchasing dynamics. Similarly, it is too early to tell whether most consumers will prefer the traditional, store-bought version of a recording or whether invisible MP3 files will suit widespread popular taste as a primary format. However, if listeners are just as pleased with an electronic version, many will still prefer to obtain it for free, as long as it is sonically indistinguishable from the "genuine" article. Underground trading will continue to occur among listeners who are not concerned about collecting and possessing official editions, especially in an era of downloadable recordings, which, by their nature, need not include accompanying artwork or other packaging. Record companies will need to find a way to persuade listeners to prefer commercial music files to infringing versions, be they downloaded from a pirate site, located through Napster or something analogous, or just a copy of a friend's original CD source. Out-of-print material will still be otherwise hard to find in an official version, however.[124]

Copyright holders will continue to face an uphill battle in trying to sink MP3 pirates, especially when the latter are international rogues who might be anywhere and who will persist. In order to thrive in the twenty-first century, the antipiracy cause will continue to need more and high-profile criminal enforcement as a deterrent (including crackdowns on the supply side); more and efficient civil causes of action for victims of infringement; more and stepped-up implementation of ever-evolving technology standards for security; harmonization of international treaties and laws; clarification as to issues of jurisdiction in cyberspace; trade sanctions against nations that do not adequately respond to piracy within their borders; and far better copyright law education of the Internet-using public. Ultimately, the public must be disabused of the ignorant mentality that "anything goes" on the Internet, and that "information wants to be free."[125] Proprietary information does not want to be cost-free.

Significant antipiracy progress is in reach, but no single measure will be perfect. Without doubt, the revolution will be downloadable; history tells us that it will be pirated, but the degree remains to be seen. Eventually, far more computer users will have access to higher-speed equipment and Internet connections. Once online-available music is truly technically secure (presuming that the prospect is realistic), most honest consumers ideally would find it no less feasible to pay a reasonable amount for an expedient, quality-guaranteed, authorized download than to troll the black market of cyberspace for free files. Copyrights probably will be more technologically secure for future recordings than for works that have existed up to now. If and when MP3 becomes a more secure medium, it will flourish as the most revolutionary innovation the recording industry has seen at least since the introduction of the CD in 1983, but only until the inevitable next better alternative renders it obsolete.

Endnotes

1. An "open source" technology is one that proprietors intentionally make freely available to the public for use, without charging licensing fees.
2. A compression standard is a software technology that shrinks files for expedient storage and transmission.

3. "Codec," like "modem," is a portmanteau word. It implies "compression" and "decompression."

4. In an intellectual property context, a "pirate" is one who illicitly reproduces proprietary material to which he or she does not lay any legal claim. A pirate may or may not wish pecuniary harm to the rightful owner.

5. A copyright holder of a "nondramatic musical work" enjoys the exclusive right to control distribution, subject to "compulsory licensing" provisions. 17 U.S.C. § 106(3); 17 U.S.C. § 115. Any act that compromises the exclusive rights of copyright holders to undertake and manage these initiatives constitutes an infringement. 17 U.S.C. §§ 501 *et seq*.

6. 17 U.S.C. § 109(a). The language of this provision refers to "sell[ing] or otherwise dispos[ing] of the possession of [a] copy or phonorecord," which implies a total transfer from single party to single party, not from single party to a multitude, like the lighting of so many candles from the same fire. The latter is the nature of uploading material for unlimited download.

7. The company that runs this "peer-to-peer" exchange site (http://www.napster.com) is currently the defendant in one of the most hotly contested, and closely watched, copyright suits in recent memory, *A&M Records v. Napster, Inc.*, No. C99-5183 MHP (N.D. Cal.) The suit alleges that Napster promotes massive copyright infringement among its members. Judge Marilyn Hall Patel ordered the service shut down in July of 2000, but, as of the time of writing, Napster was still operational, having won an eleventh-hour stay in the Ninth Circuit.

8. At one point, SwapStation, http://www.swapstation.com, an interactive MP3 exchange site, implored its users to "do it legal" [sic] and actually trade their master copies rather than amass accruing, free versions. It is an unrealistic expectation, but probably a prophylactic gesture. *See MP3 Swapping Simple as 123*, (Dec. 20, 1999), at http://www.mp3.com/news. *See also* David Ignatius, *. . . And a Pirate in a Pear Tree,* Washington Post, Dec. 15, 1999 at A47.

9. At the time of writing, Napster boasts 32 million users. *See generally* Napster's press releases at http://www.napster.com/pressroom/pr/001003.html (visited Oct. 21, 2000).

10. *See* discussion of the Secure Digital Music Initiative (SDMI), *infra*.

11. The chief exception to autonomy over one's own e-mail is employers' ability to monitor their employees' transmissions conducted on workplace equipment. Privacy issues are beyond the scope of this paper, *but see* the workplace-related chapters in Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995).

12. Earlier in 2000, "MP3" was the most searched term on the Internet, but as of the time of writing, "travel" has stolen its crown. *See generally* http://searchterms.com (visited Oct. 22, 2000).

13. *See generally* Clinton Heylin, Bootleg: The Secret History of the Other Recording Industry (1996). This book is the definitive history of trade in illicit music recordings, with a primary focus on hard copies of "bootlegs," which differ from pirated copies in that they consist of unreleased material. (This paper does not focus on bootlegging as a form of copyright infringement.) Heylin disturbingly elevates to folk-hero status those who would be so disrespectful of an artist's integrity and rights as to plunder proprietary material for personal gain.

14. Piracy's effects ripple all throughout the recording and retailing industries as the result of decreased consumer demand. The public sustains economic injury in the form of lost employment and uncollected tax revenues and customs duties. *See generally* Council of European Publishing, The Fight Against Sound and Audiovisual Piracy Handbook (1995).

15. A "hacker" is a skilled computer user who uses his (or her, though usually *his*) knowledge and/or equipment for exploratory and/or nefarious purposes, such as to defeat technical security functions or to gain unauthorized access into remote locales.

16. I use the term "freeloader" to refer to those on the demand side who avail themselves of already-uploaded materials that a "pirate" has taken and made publicly available online. The two categories of actions should be distinguished. Infringement of distribution rights, for example, generally only implicates pirates, *but see* the bartering provisions in the No Electronic Theft (NET) Act, discussed *infra*.

17. The Industrial Revolution began around the turn of the nineteenth century in England, and continued soon thereafter in the United States and continental Europe.

18. I use the recording industry's term "track" generally to refer to a recording of a single song or other individualized (usually short) work.

19. *See, e.g.,* RIAA press release, "RIAA Releases 1999 Midyear Anti-Piracy Statistics," Aug. 17, 1999, at http://www.riaa.com; William Bastone, *Pirate King: Music's No. 1 Bootlegger Gets Busted—Again,* Village Voice, Feb. 23, 1999, at 43; Sarah Saffian, *Yo-Ho-Ho and a Stolen Video!*, Daily News, July 5, 1995; Elizabeth Corcoran, *In Hot Pursuit of Software Pirates,* Washington Post, Aug. 23, 1995, at F1.

20. *See generally* Matt Richtel and Sara Robinson, *Ear Training: A Digital Music Primer*, July 19, 1999, N.Y. Times, at C6, describing digital music as "not any one thing, but rather a continually mutating set of technologies by which sounds can be made, captured, and passed around invisibly . . . don't presume [the principal formats will] be the same a year, a month, or even a week from now." For a preview of AAC ("Advanced Audio Coding"), a possible successor to MP3 as a compression standard, *see also* http://www.mpeg.org/MPEG/aac.html.

21. "Digital phonorecord delivery" (DPD) is the term coined in the Digital Performance Right in Sound Recordings Act of 1995 (DPRSRA) to describe "each individual delivery"of a digital file such that the recipient winds up with a reusable copy, as distinguished from an ephemeral "transmission," such as a "streaming," online radio broadcast. 17 U.S.C. § 115(d). A download of a music file from an unauthorized Web site fits this description because of the residual, reusable content thus arriving on the user's hard drive. The definition leaves room to argue that each download-hit on an infringing site constitutes an individual count of unauthorized distribution, a key consideration in the once-interpreted No Electronic Theft (NET) Act (*see infra*), which contemplates the aggregate dollar value of infringing material. Anyone who uploads another party's proprietary music files without a DPD license (as granted by the Harry Fox Agency, *see infra* note 39) and who does not pay the statutory rate per instance is pirating. For an expansive discussion of rights in digital music, mostly beyond the scope of this paper, *see generally* Bob Kohn, *A Primer on the Law of Webcasting and Digital Music Delivery* at http://www.kohnmusic.com/articles/newprimer.html (visited Oct. 18, 2000). Cohn is the Chairman of eMusic (formerly known as GoodNoise) and the former chief counsel to Pretty Good Privacy.

22. "Ripping" is the process of copying the binary code from a CD and loading it into a computer, via the CD drive, for conversion to a new format.

23. "Encoding" is the term used for the process of converting binary data to the MP3 format. AudioCatalyst, for example, both rips and encodes data for Macintosh as well as Windows platforms. *See* http://www.xingtech.com/mp3/audiocatalyst.

24. "Burning" is the process of recording data onto a blank compact disc, analogous to making a tape recording or taking a photograph. It involves an apparatus called a "burner."

25. *See generally* Neil Strauss, *Free Web Music Spreads from Campus to Office*, N.Y. Times, Apr. 5, 1999, at A1.

26. The name is short for Motion Picture Experts Group-1 Audio Layer 3. The Motion Picture Experts Group, or "MPEG" (pronounced "EM-peg") is a family of standards for compressing digital audio and video signals. Its joint direction comes from the International Standards Organization (ISO) and the International Electro-Technical Commission (IEC). *See* http://www.mpeg.org. *See also* "Frequently Asked Questions about MPEG Audio AAC," http://www.iis.fhg.de/amm/techinf/aac/aacfaq/index.html.

27. *See* http://www.fhg.de/english/company/index.html.

28. *See* Gerry Blackwell, *Squeeze Play,* Toronto Star, Aug. 12, 1999, for an apt comparison of compressed digital audio signals to orange juice concentrate.

29. *See* Larry Lange, *MP3 Compression Opens Recording Industry to Hackers—Net Pirates Plunder the High Cs*, Electronic Engineering Times, July 21, 1997.

30. *Id.*

31. *See* Ted Greenwald, *Inside Encoding.com,* Wired, Aug. 1999, at 142.

32. *See supra* note 22.

33. In these bulletin board-like hideouts, users can anonymously place and fulfill individual requests for specific songs, as though in a free restaurant, while their comrades seem to serve up their own potluck specials at leisure. A search of Usenet newsgroups on December 22, 1999 (relatively early in the Napster period) revealed seventeen dedicated areas with MP3 in their names. *See, e.g.*, alt.binaries.sounds.mp3.requests, alt.binaries.sounds.mp3.nospam, or, alt.binaries.sounds.mp3.1990s.

34. A "chat room" is an online forum where many Internet users can gather at once, often anonymously, to communicate with each other in real time about a particular subject.

35. Downloadable at http://www.winamp.com.

36. Downloadable at http://www.macamp.net.

37. A "search engine" is an interactive Web site that locates requested information on the Internet based on key words.

38. Lycos's disclaimer is upfront about the likelihood of tracking down unauthorized material online:

> When accessing MP3 files on the Internet, you are accessing content over which Lycos and FAST have no control. The content in those files is determined entirely by other parties who make those files available on the Internet, and those other parties are solely responsible for such content. Lycos and FAST have no control over that content and have NO responsibility for such content. Rather, Lycos and FAST are merely providing access to such content as a service to you. Lycos and FAST expect all who use the Internet to abide by all laws, including all copyright and other intellectual property laws. It is the policy of Lycos and FAST to respond expeditiously to claims of intellectual property infringement.

http://mp3.lycos.com/disclaimer.html.

39. The Harry Fox Agency (HFA) is the licensing and royalty-collecting subsidiary of the National Music Publishers' Association (NMPA), which is to the distribution of sound recordings what the American Society of Composers, Authors and Performers (ASCAP) (http://www.ascap.com) is to public performances of them. It is the principal trade association for music publishers and represents over twenty thousand members in the United States.

40. Press release, *The Harry Fox Agency, Inc. and Goodnoise Corporation Enter into MP3 Digital Phonorecord Delivery License Agreement,* Feb. 3, 1999. http://www.nmpa.org/pr/goodnoise.html. (This article does not address digital phonorecord delivery's cousin forms of online audio, such as "streaming" or "webcasting," which are quasi-real-time transmissions that do not result in an enduring copy at the receiving end. Their distribution and licensing implications vary somewhat from those of DPDs and will be the subject of a future paper by the author.).

41. A "wav" (pronounced "wave") is sound file in a common, Windows-compatible format.

42. *See, e.g.*, Chris Stamper, *Blame It on Rio,* Oct. 16, 1998, http://www.abcnews.com. The sound of some MP3 files is so crisp, however, that the difference is negligible or even unnoticeable when played through headphones.

43. A "CPU," short for "central processing unit," is the main brain of a desktop computer, in which the memory is stored and in which electronic operations are carried out.

44. *See* Christopher Jones, *MP3s Anywhere You Are* (Oct. 28, 1999), at http://www.wired.com/news.

45. *See, e.g.*, Michel Marriott, *MP3 Goes on the Road: A Digital Player for the Car,* N.Y. Times, Oct. 28, 1999, at G3.

46. Most CDs these days are not brimming with equally appealing songs. They might contain, for example, two or three hits and nine or ten non-starters, analogous to what used to be called "B sides" in the days of the 45-rpm vinyl single.

47. "CD-Rs" are user-recordable compact discs. They are analogous to, but still far less common than, blank cassette tapes. A single CD-R, which costs less than two dollars, can store hundreds of MP3 song tracks in its 650 MB capacity. Greg Michetti, *Revolution the Portable Audio,* Toronto Sun, May 28, 1999, at C7.

48. A "T1 line" is a high-speed, high-bandwidth, leased line connection to the Internet. T1 connections deliver information at 1.544 megabits per second. *Netdictionary* at http://netdictionary.com (visited Oct. 21, 2000).

49. A "T3 line" is a high-speed, high-bandwidth, leased line connection to the Internet. T3 connections deliver information at 44.746 megabits per second. *Netdictionary* at http://netdictionary.com (visited Oct. 21, 2000). This is the mode of connection that SUNY at Buffalo provides, for example. (Author's personal telephone inquiry to SUNY at Buffalo's CIT Help Desk, Oct. 19, 2000).

50. *See, e.g.*, Patti Hartigan, *Byrd Man Sees Promise of Digital Music,* Boston Globe, July 14, at D1.

51. Market research firm Forrester Research projects 1999 sales of the devices to be in the neighborhood of one million units, and for thirty-two million to exist by 2003. Like VCRs and calculators before them, their prices will probably fall (from the current $200 and above) if and when they catch on. *See, e.g.,* Frances Katz, *Music Industry Embraces Net,* Atlanta Journal and Constitution, June 30, 1999, at 5D. *See also* Gerard Grach, *Support Your Local MP3,* New Media Age, June 17, 1999, at 12.

52. No. 98-56727, 1999 U.S. App. LEXIS 13131 (9th Cir. 1999).

53. 17 U.S.C. §§ 1001-1010.

54. *Id.* § 1008. This pre-MP3-era provision could be more specific about what a consumer may do with such homemade copies. The drafters appear not to have foreseen the brisk phenomenon of unauthorized MP3 distribution in the forms of posting and trading. (The statute may mislead some to believe that they may make as many copies as possible and then distribute them to, and trade them with, others however they please.).

55. *Id.* § 1002.

56. The act defines "serial copying" as the duplication in a digital format of a copyrighted musical work or sound recording *from a digital reproduction* of a digital music recording." 17 U.S.C. § 1001(11), (emphasis added).

57. 17 U.S.C. §§ 1003-1004; §§ 1005-1007.

58. *See* http://www.diamondmm.com.

59. "Space shifting" is the process of moving a recording from one medium or format to another. It is the physical counterpart to "time shifting," a concept articulated in *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). The Audio Home Recording Act (AHRA) permits such qualified use.

60. During the pendency of the litigation, RIAA president Hilary Rosen said of the device, "What they call a file transfer is really a copy." *See* Chris Stamper, *Blame It on Rio,* Oct. 16, 1998, http://www.abcnews.com.

61. Inevitably, however, hackers have posted code that would allow retrograde transmission of data from a Rio back to a hard drive, inconsistent with the intended use of the device. *See* Robert Wright, *MP3 News Moving Fast and Furious,* Toronto Star, Feb. 18, 1999.

62. Title II, Pub. L. No. 105-304, 201, 112 Stat. 2860.

63. 17 U.S.C. § 1201.

64. *See* discussion of the Secure Digital Music Initiative (SDMI), *infra*.

65. 17 U.S.C. §§ 512 *et seq*. This procedure is known as "notice and takedown."

66. *See* Recording Industry Association of America, *Soundbyting Top 10 Myths* at http://soundbyting.com (visited Oct. 21, 2000).

67. 17 U.S.C. § 512.

68. *See* http://www.loc.gov/copyright.

69. "Bandwidth" is "the amount of information or data that can be sent over a network connection in a given period of time. Bandwidth is usually stated in bits per second (bps), kilobits per second (kbps), or megabits per second (mps)." *Netdictionary* at http://netdictionary.com (visited Oct. 21, 2000).

70. *See, e.g., infra* notes 90-91.

71. Paul Goldstein, Copyright's Highway 187 (1994).

72. *Id.*

73. *See, e.g.,* Sara Robinson, *Researchers Crack Code in Cell Phones,* N.Y. Times, Dec. 7, 1999; Yuzo Saeki, *Hacker Delays Launch of New DVD Machines in Japan,* Reuters, Dec. 3, 1999. *See also infra* note 118.

74. Codified throughout 17 U.S.C. and 18 U.S.C.

75. U.S. Department of Justice's summary of the statute at http://www.usdoj.gov/criminal/cybercrime/netsum/htm (visited Oct. 21, 2000).

76. 17 U.S.C. §§ 506 *et seq.*; 18 U.S.C. §§ 2319 *et seq*.

77. A "bulletin board system," or "BBS," is a specific dial-up locale whereby users can communicate with each other or post or access content. It was a popular Internet medium before the 1990s advent of the World Wide Web and thus today's ubiquitous "Web site."

78. *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994).

79. 17 U.S.C. §§ 101 *et seq.*

80. 18 U.S.C. § 2319A(d)(2)(c).

81. The court also originally barred Levy from using the Internet during the period of his probation but changed its stance when Levy asserted that he needed it in order to complete his thesis. Software and Information Industry Association of America, *First Software Pirate to Be Convicted and Sentenced Under 1997 Net Act*, at http://www.siaa.net/piracy/news/jefflevysentence.htm (visited Nov. 24, 1999).

82. *See generally* U.S. Department of Justice press release, *Defendant Sentenced for First Criminal Copyright Conviction Under the 'No Electronic Theft' (NET) Act for Unlawful Distribution of Software on the Internet* (Nov. 23, 1999), at http://www.usdoj.gov/criminal/cybercrime.

83. In the course of just two hours, the site put out 1.7 gigabytes (GB) of data, which was typical of its volume. Andy Patrizio, *DOJ Cracks Down on MP3 Pirate* (Aug. 23, 1999), at http://www.wired.com/news.

84. *Id.*

85. U.S. Department of Justice press release, *Defendant Sentenced for First Criminal Copyright Conviction Under the 'No Electronic Theft' (NET) Act for Unlawful Distribution of Software on the Internet* (Nov. 23, 1999), at http://www.usdoj.gov/criminal/cybercrime.

86. Many of today's MP3 pirates and freeloaders do not have, and will never have, any other criminal record. Many are suburban and middle-class, and many are minors.

87. *See* Doug Bedell, *As Millions Download Music off the Net, Piracy Enforcement Flounders,* Dallas Morning News, July 27, 1999, at 1F.

88. To report unauthorized trafficking in MP3 music files, one can telephone (800) BAD-BEAT or leave an e-mail tip at Badbeat@riaa.com.

89. *See* Lou Carlozo, *ABCs of MP3,* Chicago Tribune, Apr. 11, 1999, at 1C.

90. For example, SUNY at Buffalo

> does not monitor or generally restrict material residing on [its own] computers housed within a private domain or on non-University at Buffalo computers, whether or not such computers are attached to campus networks." However, in the event that a student is found to have trafficked illegally in unauthorized material, he or she "will be subject to the existing student or employee disciplinary procedures of the University at Buffalo. Sanctions may include the loss of computing privileges. Illegal acts involving University at Buffalo computing resources may also subject users to prosecution by State and federal authorities. . . .

See http://wings.buffalo.edu/computing/policy/Com_Net_Usage.html.

91. For example, SUNY at Buffalo "reserves the right to remove or limit access to material posted on university-owned computers when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated, *but does not monitor the content of material posted on university-owned computers."* (emphasis added). However, the school's policy expressly calls for a user to obtain "written permission from the copyright holder . . . to duplicate any copyrighted material. This includes duplication of audio tapes, videotapes, photographs, illustrations, computer software, and all other information for educational use or any other purpose." *Id.*

92. *See generally* http://www.soundbyting.com.

93. Author's telephone inquiry to RIAA's antipiracy unit, Oct. 25, 2000.

94. *Id.*

95. *See, e.g.,* Doug Reece, *Co-eds Busted in MP3 Crackdown* (Nov. 8, 1999), at http://www.mp3.com/news.

96. Privacy rights are beyond the scope of this paper, and no such litigation was known to be under way in connection with this raid at the time of writing, but *see generally* Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995).

97. The RIAA pressed the university for the names of the students in question, but officials would not reveal their identities. *See* Doug Reece, *U. of Piracy* (Dec. 7, 1999), at http://www.mp3.com/news.

98. *Id.*

99. *See* Alice Rawsthorn, *Music Industry Launches Legal Battle Against Internet Piracy,* Financial Times, Mar. 25, 1999.

100. *Id.*

101. *Id.*

102. *See* IFPI press release, *Recording Industry Aims Global Crackdown on Internet Pirates* (Oct. 28, 1999), at http://www.ifpi.org.

103. *Id*.

104. *See, e.g., Record Industry Acts on China Pirate Websites,* Reuters, Dec. 15, 1999.

105. *See System Set to Counter Music Piracy on Net,* Daily Yomiuri (Tokyo), June 15, 1999, at 12.

106. For a complete list of member entities, *see* http://www.sdmi.org.

107. *SDMI Fact Sheet* at http://www.riaa.com (visited November 15, 1999).

108. *Id.*

109. For a more expansive critique of SDMI, *see* David E. Weekly, *Why SDMI Will Fail* (May 17, 1999) at http://www.hitsquad.com/smm/news/9905_113/. As of May 1999, Weekly was a student at Stanford University. In 1997, Weekly posted his entire music collection on his Web site on his school's server, which almost crashed because the traffic was so heavy. When Geffen Records contacted Stanford, Weekly removed the content, which he had not been authorized to post for distribution. Patti Hartigan, *The Prophet Chuck D., on MP3,* Boston Globe, Feb. 12, 1999, at E1.

110. Secure Digital Music Initiative, *SDMI FAQ* at http://www.sdmi.org (visited Oct. 21, 2000).

111. *Id*.

112. *See* SDMI press release, *SDMI Announces Standard for New Portable Devices* (June 28, 1999) at http://www.sdmi.org.

113. *See generally,* Konrad Roeder, *How Watermarks Protect Copyrights* (Nov. 4, 1999), at http://www.mp3.com/news.

114. SDMI press release: *SDMI Identifies Audio Watermark Technology for Next Generation Potable Devices for Digital Music* (Aug. 9, 1999) at http://www.sdmi.org/dscgi/ds/py/Get/File-611/sdmiaug9.htm.

115. *Id.*

116. ARIS Technologies, Inc., *SDMI Phase I Watermark Technology License Agreement* (Aug. 20, 1999), at http://www.mp3.com/news.

117. *See, e.g.,* Sara Robinson, *Researchers Crack Code in Cell Phones,* N.Y. Times, Dec. 7, 1999; Yuzo Saeki, *Hacker Delays Launch of New DVD Machines in Japan,* Reuters, Dec. 3, 1999.

118. At the time of writing, SDMI had just run a contest to see whether any of six security codes could stand up to hackers, and it was evaluating claims by several entrants who alleged that they had cracked these systems. Benny Evangelista, *Hacker Contest Won't End Music Debate,* San Francisco Chronicle, Oct. 16, 2000, at D1.

119. eMusic now sells downloadable recordings for $.99 per song track, and $8.99 per full-length CD. These prices are embarrassingly competitive for the consumer market and reflect the absence of several levels of middlemen in the supply chain. *See generally* http://www.emusic.com.

120. *See* Steven V. Brull, *Are Music Companies Blinded by Fright?* Business Week, June 28, 1999, at 67; *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

121. Dominic Rushe, *Music Makers Seek Harmony on the Net,* Sunday Times (London), July 11, 1999.

122. Bruce Haring, *On-line Music May Play to the Tune of $1.1 Billion,* USA Today, Apr. 12, 1999, at 1D, citing that day's report by Forrester Research.

123. *See* Chris Oakes, *Research: Sell MP3s Sell CDs* (July 19, 1999) at http://www.wired.com/news.

124. Of course, MP3 piracy of out-of-print recordings will continue if such material remains otherwise unavailable.

125. This saying is attributed to *Whole Earth Catalog* founder Stewart Brand, but see where Brand crucially completes his philosophy in Joel Garreau and Linton Weeks, *AOL: Love at First Byte; Visions of a World That's Nothing But Net,* Washington Post, Jan. 11, 2000, at C01: "Yeah, I said that . . . But nobody remembers the second line, which is 'Information also wants to be expensive.' That's the paradox that drives this thing."

David R. Johnstone is a third-year student at SUNY at Buffalo Law School. **He would like to thank Professor David R. Koepsell for guidance in the preparation of this article, a version of which won Second Prize in the 2000 Intellectual Property Law Section Law Student Writing Contest.**

Trade Secrets and the Internet: How to Avoid Disaster

By Victoria A. Cundiff

I. Introduction

The CIA has announced that its release of hundreds of intelligence reports on its Internet site for Gulf War veterans before adequately reviewing them for national security issues had done "serious damage to intelligence sources and methods." But it has concluded that it is too late to do anything about it. "Many Gulf War veterans had already copied them [from the Web site], and a private Washington publishing house defied Pentagon and CIA officials and released the entire set of documents on its own Internet site."[1]

The Canadian government was embarrassed this year to discover that one of its military's top-secret electronic eavesdroppers had posted on his individual Web page the names, photos, and location of CF-18 pilots based in Italy before and during the war in Yugoslavia, along with details of his duties.[2] The Canadian Defense Department also made available on its own Web site a list of personnel working with its electronic espionage agency.[3] Analysts expect that the information has probably been downloaded by "every intelligence agency in the world."

Such disasters could happen to you. The Internet, at least in its public access areas, is no place for secrets. Some commentators estimate that as many as 150 million people can access the Internet worldwide. Scores of millions of people access it routinely in the United States alone. These viewers all can examine, download, copy, and broadly retransmit both publicly posted information and e-mail directed to them personally without the knowledge of the owner of the information.

To qualify for protection as a trade secret, information must be kept secret. A trade secret "derives independent economic value, actual or potential, from not being generally known to" others and "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[4] "Matters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret."[5] Clearly, then, there is an almost deadly tension between the Internet and trade secrets. The Internet can destroy trade secrets almost instantaneously by exposing them to millions of viewers. And, indeed, even if a secret is removed from online, a "cached" version of the text incorporating the secret may remain resident in search engines for months to come. It could remain on viewers' hard drives forever.

This article will focus on practical tips to prevent release of secrets on the Internet, consider the legal consequences of disclosure on the Internet, and ponder what to do if the worst happens.

II. Losing Secrets on the Internet

It is easy to understand why secrets can be destroyed on the Internet. Making a secret publicly available to potentially millions of viewers is inviting trouble. But how can secrets get on the Internet in the first place? Several ways:

- Companies actually post them deliberately, with no thought for, or understanding of, the consequences. Examples include Web sites listing the company's new sales contracts and strategic visions for the future or incorporating or revealing the company's proprietary software or new product plans. The CIA's hurried but unreviewed posting falls into this category.
- Companies post their secrets carelessly. Thus, for example, marketing personnel may post details about products under development without clearing the posting with the personnel actually developing the new products.
- Employees e-mail secrets to third parties for legitimate business purposes, but with inadequate precautions against retransmission. Third parties thereafter can freely (or accidentally) retransmit them to countless others over the Internet, either via directed e-mail or via public posting accessible by wide segments of the public.
- Employees deliberately e-mail secrets to third parties to spirit them out of the company. E-mail is a far more efficient, and sometimes less detectable, way of removing secrets than carrying out boxes of documents in the dead of night. In a much publicized California suit, for example, Cadence Corporation has alleged that this is precisely how its competitor, Avant!, gained a competitive advantage at Cadence's expense. Two of the recent convictions under the Federal Economic Espionage Act stemmed from e-mail transmissions or Internet offers to sell trade secrets.
- Employees or others publicly post secrets for the express purpose of sabotaging the company owning them. Such activity has been alleged in suits

brought by Raytheon, Ford Motor Company, and an affiliate of the Church of Scientology, among others.

- "Hackers" gain entrance to a company's internal computer system or intranet and access and copy stored secrets.
- Cyberspies develop other means to access trade secrets without detection.

Each of these potential threats to trade secrets presents different legal issues and requires different preventive measures.

III. Steering Past Trouble

A. Web Pages: Postings You Control

Many corporate Web sites are essentially extended corporate advertising, intended to provide consumers and the public with information about the company, its employees, products, and business plans. Companies need to insure that the information they provide on their Web sites does not include trade secrets.

Web sites typically are designed by or for companies. From both a practical and a legal standpoint (at least in the trade secrets context), therefore, the company has control over what appears on its Web page. The company should exercise this control with an eye to taking reasonable measures to protect trade secrets.

Keep in mind that it is not only potential customers who view Web sites. Actual competitors do, too.[6] Listing satisfied customers with whom the company has an ongoing relationship may strike an advertising agency as an important way of demonstrating the company's success. Indeed, it may be the best way. But that way will also almost certainly destroy the company's ability to argue in another context that those customer identities and those particular contracts are confidential. By posting them on the Web page, the company took *no* let alone "reasonable" precautions to maintain secrecy.[7] Perhaps the central message—that the company has satisfied customers in many geographic and business sectors—could be powerfully conveyed in another way with less risk to corporate secrets.

Similarly, if a company wants to be in a position to argue that knowing which employees have particular capabilities or are members of a particular development team is confidential information to be protected from recruiters, the company should not post such details on its Web site.

Making sure that corporate personnel who are familiar with what secrets the company wishes to protect review Web postings *before* they are posted is a sound precaution. In many companies, it makes sense to consider review by representatives of several parts of the organization, since marketing, sales, and research and development groups may not all be equally attuned to protecting each other's secrets. This approach should reduce the risk of the "rush to post" syndrome that plagued the CIA. Similarly, in the case of franchises, requiring the franchiser to approve any Web pages franchisees wish to establish is also a practical safeguard.

Reviewing personnel should also be mindful that the secrets of others should not be displayed on the company Web page, either. While the company owning the Web site may not mind displaying its customer list, for example, the customers themselves may want to keep their source of supply secret. When in doubt, check before posting information others can claim to be confidential.

B. Web Site Development Considerations

Keep in mind that Web sites display not only words. To the initiated, they also can reveal the source code for the software generating the exciting graphics displayed on Web sites. This fact means that Web watchers may be in a position to duplicate those graphics for others, diluting their visual distinctiveness. How to prevent this risk? A legend reserving all rights in the software may help from a legal standpoint, as will a copyright notice. Depending on the nature and value of the software, such a warning may occupy an entire page and may require the viewer's affirmative assent before permitting further access. But such a warning may not fully protect the ideas underlying the software—the domain of trade secrets—as opposed to the specific expression incorporated in the software—the copyright.

One practical way of protecting most of the software used in connection with a Web site is to write it in a manner that does not display the entire program. Many programs can be written so that all that appears in code visible on the Internet is a series of instructions to merge in files or other programs in response to some action by the user. These other programs, which actually create the graphics, are typically not visible on the Web site and are not downloadable. They are instead executed on the Web server itself and therefore never get into the hands of those who would copy them. This precaution is something Web site developers—and companies who commission them—should keep in mind.

Remember, too, that new software poses new challenges. Java® software, for example, embeds executable program code into downloadable Web materials. While reverse-engineering such code is currently very difficult, making it a good choice for protecting proprietary programs, over time that may change. And over time, those using such software without clearly establishing

that the viewer has assumed a duty of confidentiality may be found to have taken inadequate precautions to maintain secrecy. Thus new precautions may need to be taken to prevent future leaks.

Finally, to the extent third parties are involved in creating a Web page, the site owner should gain ownership of all appropriate software (a matter that will typically be the subject of negotiation, since the developer may wish to reuse certain core software to write or drive other software he or she writes in the future) and require all who participated in developing the page to sign appropriate confidentiality and transfer agreements. While such agreements cannot protect as secrets information actually appearing without confidentiality controls on the Web page, they may protect both information and concepts underlying the display or pertaining to future plans. The site owner also should gain the developer's promise to keep confidential all business information the company may show the developer during the course of the engagement.

C. E-mail: Transmissions You Can Safeguard

Increasingly, many people use the Internet primarily as a form of fax machine to e-mail communications to specific recipients. While some people (generally those not well-versed in the way the Internet works) fear that "beaming" transmissions exposes them to interception by the public, and thereby destroys their secrecy in the same way that some cellular telephone equipment does, there are in fact extremely important technical differences between the two transmissions. Cellular telephones are a form of radio. This means that, at least in the early analog form still used in many parts of the country, cellular signals can be readily intercepted by receivers operating on the same frequency as the transmitter. This is why so many people have had the experience of hearing tantalizing bits of information transmitted via cellular phone in the midst of a conventional phone call or television or radio program.

The Internet is different. While the wrong person can indeed receive an e-mail, in the first instance that fact stems not from e-mail technology but rather from human error in mistyping the e-mail address—a problem that can just as well arise with faxes or conventional mail. A legend advising that improperly directed or received e-mails should be destroyed *and deleted* may persuasively be argued to serve as a reasonable precaution to maintain the secrecy of such misdirected e-mail.

One can make the argument that even unencrypted Internet e-mail is generally more secure from interception than other forms of communication because of the way the Internet works. Information transmitted over the Internet, as opposed to e-mail sent by services such as America Online, CompuServe, or MCI Mail, is not transmitted as a constant stream of information.[8] Instead, it is broken into small "packets" of data, each of which typically reaches its final destination via a different path. Some packets may travel from New York to Washington via Bangkok, for example, while others may travel through Toronto. These packets are reassembled into a single message only at the end of their travels. The precise route traveled typically varies from message to message. This is part of why the time for e-mail transmission can vary so widely—different messages may travel by very different routes. (This complex routing was initially developed to prevent a communications breakdown if a primary communications node was destroyed in a military disaster.)

This transmission method means that in fact in most cases it is unlikely that e-mail messages will be any more readily intercepted than other more familiar means of communication. Moreover, interception of e-mail being transmitted over the Internet is unlawful under the Electronic Communications Privacy Act. Interception of *stored* e-mail, however, appears to fall outside the scope of this Act, a fact suggesting the need to password protect highly sensitive e-mail so that once received it cannot be widely accessed.[9]

These facts, while offering substantial comfort, do not mean that use of the Internet to transmit trade secrets poses no risk. Companies desiring to use e-mail to transmit sensitive information internally would do well to construct an "intranet" with a secure firewall preventing against potential retransmission over the external Internet. This type of communication has been held by courts to maintain a reasonable expectation of privacy.[10]

The primary risk of transmitting confidential information over intranets or the Internet, however, lies not in the mechanics of transmission, but rather in the fact that once digitized information is transmitted via e-mail, it can then more readily be re-transmitted by the recipient to larger numbers of unauthorized people than is true with more conventional means of communication. A vendor can with a few key strokes e-mail the customer's pricing parameters to the customer's competitors. A scientist can e-mail the formula to others secretly working on a competing product. And the disgruntled colleague can e-mail the communication to discussion groups, which are discussed in greater detail below, that will then automatically transmit and retransmit and exchange the information with countless other discussion groups throughout the world.

How can these threats be reduced? By using intra- and extranets to limit the universe of potential recipients of confidential information. By counseling employees and others to use caution in selecting what they transmit over the Internet (is it really necessary from a business standpoint?), in selecting intended recipients

(do they truly need to know the information? have they executed a confidentiality agreement? have they been reliable in the past? have they been apprised that this particular information is confidential?), in accurately addressing e-mail, and in implementing protective measures such as password protection and encryption that both underscore the importance of the confidentiality obligation and make it more difficult to retransmit the message to third parties. And by conducting periodic tests to see if company-mandated safeguards are in fact being followed, or need to be strengthened.

It has been argued that with the increasing availability of reasonably priced and largely effective encryption software, failing to use it may evidence a failure to use what has become a reasonable measure to maintain secrecy.[11] One need not go so far as to embrace this conclusion, however, to understand that using such protective measures certainly send the clear message "this secret is not free to take or spread."[12]

Companies can take other practical measures to prevent excessive or inappropriate use of e-mail to transmit secrets. First, many communications need not be made over the Internet at all. If the intended recipients all work at a single organization, the information may be easily conveyed via a local network or "intranet".[13] Second, many companies do not give all employees Internet access for a variety of reasons, including security. If something needs to be e-mailed via the Internet, it must be given to a supervisor who reviews the need to transmit it.

Third, sophisticated monitoring software is becoming increasingly available to track what happens to particular documents, including whether they are forwarded to others, downloaded, copied, or e-mailed. Such software should be used in environments in which there is a high concern for security. Reports should be reviewed frequently as to particularly sensitive information, and certainly in connection with the departure of employees who have had access to highly confidential documents. They may pinpoint trouble. In the highly publicized departure of José Ignacio Lopez from General Motors, for example, it was alleged that shortly before his departure Lopez had transferred massive amounts of GM's secrets from the U.S. to Germany over GM's internal e-mail system and then accessed them with Volkswagen's computers. Appropriate electronic "tags" on the these documents might have alerted GM to the problem earlier—even a simple count of the mammoth number of megabits e-mailed from computers under Lopez's control would have done so. Even the records that did exist were central to GM's prosecution of the case.

Similarly, in connection with a key Borland employee's departure to Symantec, copies of the employee's e-mail to Symantec in the days prior to his departure formed the basis for a criminal suit, later dismissed, alleging trade secret misappropriation.

Sophisticated monitoring techniques are not always essential. An e-mail misdirected from one co-conspirator to her boss rather than to her confederate expressing nervousness that what she was doing was wrong and "really like stealing" alerted IDEXX that its trade secrets were being e-mailed out of the company and led to conviction of the confederate under the Economic Espionage Act.[14]

D. E-mail Transmissions by Lawyers

At least one state bar, Iowa, had initially concluded that the risk that e-mail will be intercepted is such that before lawyers can send "sensitive information" via e-mail, they must either obtain written consent and acknowledgment of the potential risk of a confidentiality breach or encrypt, password protect, or otherwise protect the information transmitted.[15] However, Iowa has rethought that conclusion and issued a new determination amending the earlier opinion. The new opinion, which is only available to Iowa Bar members having a password permitting them to access the opinion, apparently provides that these restrictions should apply only to "sensitive" material, rather than pure exchanges of information or legal communication with clients.[16] South Carolina has also reversed its earlier opinion[17] concluding that since its earlier opinion was released, "The use of e-mail has become commonplace, and there now exists a reasonable level of 'certainty' and expectation that such communications may be regarded as confidential, created by improvements in technology and changes in the law."

ALAS, one of the country's largest malpractice insurers, has concluded that lawyers may ethically "communicate with or about clients on the Internet without encryption." This is so in part because interception of such messages would have to be intentional and, necessarily, unlawful.[18] A number of states have accepted the ALAS approach, stating that in most cases the transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules absent unusual circumstances.[19] The measures Iowa previously had imposed, however, may well be sensible measures to follow to limit the further transmission of trade secrets, for the reasons discussed below. New York's warning that

> in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use

> only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail

is also good advice.

E. Repelling Extraordinary Measures to Intercept Secrets

As technology develops, so do methods to intercept, copy, "sniff," and "spoof" to gain unauthorized access to e-mail messages. Similar techniques exist for intercepting conventional telephone transmissions. While no e-mail system is "interception-proof," in most circumstances one following the procedures outlined above should find the actual risk to be small. ALAS, a major malpractice insurer, has concluded: "To identify one of the relevant computers over which an e-mail message will pass and then locate, isolate, and capture a particular message would take a substantial investment in time and money—not to mention personnel who are both technically proficient and willing to violate the law."[20]

F. Discussion Groups: The Danger Zone

Another "lane" on the information superhighway is the discussion groups, started by various groups soliciting e-mails expressing comments on topics ranging from particular products or companies (snapple.com), to the occult (alt.magic), to current events (alt.abortion), to sports (rec.sports.boxing). This is one of the places where secrets can be put at greatest risk. If a secret gets into a discussion group, the trade secret owner has effectively lost control of it. Not only can every member of the discussion group at least theoretically access the secret for some period of time; even worse, many discussion groups automatically exchange postings with other groups. Thus a single posting of a secret can, in time, lead to its replication throughout the Internet. This fact—the total loss of control over information—is what gives most trade secret owners the greatest fear about the Internet. With good reason.

As a result, improper posting of secrets to the Internet has already led to litigation, and is likely to lead to more in the future. The initial round of such litigation often focuses on identifying the party making the unauthorized postings. Raytheon, for example, in a much publicized case, sued seeking an injunction against further posting of Raytheon secrets by 21 unidentified Internet users who had posted confidential engineering information in chat rooms and bulletin boards.[21] One of the critical initial strategies was to subpoena the Internet Service Provider Yahoo to divulge the identities of the posters. Yahoo complied.[22] Several posters subsequently resigned as Raytheon employees; others entered corporate counseling. Raytheon then dropped the suit. The fate of the postings at issue has not been discussed in press accounts.

The next issue is obtaining relief. Typically, the trade secret owner would seek an injunction requiring the trade secret to be removed and further postings of secrets to be banned. While such relief is entirely consistent with that afforded in cases of trade secret misappropriation by conventional means, at least one recent case has concluded that, absent the misappropriator's breach of a contractual or fiduciary duty, an injunction against such a posting is an impermissible prior restraint on protected speech.[23]

The district court in *Lane* recognized that the posting constituted misappropriation of trade secrets and might even be criminally actionable. It nonetheless concluded that the Sixth Circuit's decision in *Procter & Gamble Co. v. Bankers Trust Co.*,[24] refusing, on First Amendment grounds, to enjoin the publication of information the parties had incorrectly stipulated in a lawsuit was "confidential," prohibited an injunction against disclosure of trade secrets. *Lane* is startling, since it appears to ignore the fact that free disclosure of a trade secret destroys the trade secret owner's property rights. The "speech" at issue is in fact what courts sometimes call "speech plus." It wrecks destruction of property.[25] Regardless of whether *Lane* remains good law or is adopted in other forums, the decision underscores the importance of keeping trade secrets away from Internet discussion groups.

Obviously, anyone who has access to trade secrets should be counseled—but should not need to be—not to post any secrets to public discussion groups. What are the legal consequences if they do? First, consider the person who originally posts a secret to a discussion group. Assuming he or she had no authorization to do so, that person is liable for trade secret misappropriation and all the consequences thereof—including damages for the destruction of the secret. The unauthorized poster also may have criminal liability, under either the Economic Espionage Act[26] (making electronic transmission of trade secrets a crime) or other statutes.[27] Third parties acting in concert with the misappropriator may also be barred from using or retransmitting the secret.[28] But what of innocent third parties? Are they entitled to use with impunity a secret that has been posted on the Internet under the theory that it is secret no longer? Some courts have said yes.[29] In an early ruling in the case, Judge Whyte wrote in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[30]:

> The court is troubled by the notion that any Internet user, including those using "anonymous remailers" . . . to protect their identity, can destroy valuable intellectual property rights by posting

> them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. . . . Nonetheless, one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers, . . . can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation. . . . Although a work posted to an Internet newsgroup remains accessible to the public for only a limited amount of time, once that trade secret has been released into the public domain there is no retrieving it.

But this automatic conclusion that if information has been posted on the Internet it is no longer a secret does not comport with settled trade secrets law. Unlike the patent field, where the existence of a single, though obscure, reference anywhere in the world can destroy novelty, and hence patentability, the test for trade secret status is whether the information is in fact generally *known*.

Does general availability on the Internet equate with being generally known? Not necessarily. If one blares a trade secret over the loudspeaker in Yankee Stadium off-season and no one hears it, is it still a trade secret? Perhaps. In reconsidering his earlier decision that its posting on the Internet necessarily destroys a secret, Judge Whyte stated:

> [T]he Court believes that its statement in its September 22, 1995 order that "posting works to the Internet makes them 'generally known' to the relevant people" is an overly broad generalization and needs to be revised. The question of when a posting causes the loss of trade secret status requires a review of the circumstances surrounding the posting and consideration of the interests of the trade secret owner, the policies favoring competition, and the interests, including first amendment rights, of *innocent* third parties who acquire information off the Internet. . . . [T]he general public is not the relevant population for determining if a claimed trade secret is generally known. The relevant inquiry is whether the documents for which trade secret protection is sought are "generally known" to the relevant people [namely, potential competitors]. . . .[31]

Likewise, in *Hoechst Diafoil Company v. Nan Ya Plastics Corporation*,[32] the court held that the fact that a document describing plaintiff's trade secret was inadvertently filed unsealed and remained on file for several months did not necessarily preclude trade secret protection, but observed that the situation might be different if it also had been posted to the Internet.

Judge Whyte's rejection of a per se rule that unauthorized posting destroys a trade secret was embraced this year by the Santa Clara County California Superior Court in *DVD Copy Control Associations Inc. v. McLaughlin*.[33] There, Judge Elfving granted a preliminary injunction ordering the removal of Internet postings revealing the DVD encryption code even though the postings were fairly widespread and some had been up for about three months. He concluded:

> The Court is not persuaded that trade secret status should be deemed destroyed at this stage merely by the postings of the trade secret to the Internet. . . . To hold otherwise would do nothing less than encourage misappropriators of trade secrets to post the fruits of their wrongdoings on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet.

Judge Elfving went on to conclude that the trade secret owners had moved quickly to protect their rights and that injunctive relief was appropriate.

This approach certainly argues for working to delete misappropriated secrets from the Internet as quickly and thoroughly as possible, *including* from search engine services that may not update their information "caches" frequently.[34] It does not, however, entirely solve all the important practical issues. The CIA's experience suggests that if information is particularly interesting to the audience that gains access to it, downloading and retransmitting may begin almost immediately. The same appears to have been true in the DVD context, as well and, as a result, the DVD Copy Association is now going through the costly task of establishing new encryption codes. But a "look at the particular circumstances" approach does offer the prospect that an unauthorized posting need not necessarily lead to cataclysmic loss.[35]

Aside from the question of whether a trade secret, although for a time generally *available*, has in fact become generally *known*, another principle of the law of

trade secrets may help a trade secret owner whose secret has been posted on the Internet. Under traditional legal principles a third party who acquires a misappropriated secret is not free to ignore evidence of misappropriation, whether that evidence arrives with the secret or subsequently.[36]

Thus, if a trade secret makes its way onto the Internet, a trade secret owner should consider how best to get the word out that the public is not free to use it. Any given situation may be extremely delicate—sending out postings to "ignore that valuable secret!" may not be a particularly effective way of stifling curiosity. Removing the secret from the principal places it has been posted (a browser can help identify sites) and replacing the original posting with a message to the effect that "the posting added to this site at 22:18 on January 14, 2000 by Y concerning X Corp. has been removed because it was posted without X Corp.'s permission and may contain information misappropriated from X Corp. Use or retransmission of the information contained in that posting constitutes misappropriation" may help.

G. Using the Internet to Acquire or Distribute Trade Secrets

Just as using the Internet to solicit copies of copyrighted software was held to constitute copyright infringement in *Sega Enterprises, Ltd. v. Maphia*,[37] using the Internet to solicit the retransmission or other delivery of trade secrets has been held to be "wrongful acquisition" of trade secrets under the Uniform Trade Secrets Act.[38] See also *United States v. Lange*,[39] in which an individual who used the Internet to solicit potential buyers of his employer's trade secrets was convicted for violating the Economic Espionage Act.

III. Conclusion

The thoughtful owner of trade secrets will realize that those secrets do not belong on the Internet except in controlled form and will implement strong policies and practical measures updated as technology evolves to insure that secrets do not escape.

If secrets do make their way onto the Internet, however, even briefly, the trade secret owner will work to pull them off and limit the damage. Finally, to insure that its secrets are safe, the wise trade secret owner will take periodic cruises on the information superhighway looking for signs of misuse. A good browser should point the way to any trouble.

Endnotes

1. *Gulf War Data on Internet Harmed U.S. Spy Efforts*, Report Says, N.Y. Times, Aug. 8, 1997, at A15.
2. *Military Secrets Posted on Web by CP*, Calgary Sun, Aug. 26, 1999.
3. *Canadian Intelligence Security Reviewed Amid Internet Spy Furor*, Globe and Mail, Aug. 27, 1999.
4. Uniform Trade Secrets Act § 1 (adopted in more than 43 states).
5. Restatement (First) of Torts, Section 757, comment b (1939).
6. Indeed, a review of competitors' Web sites can be an excellent start in conducting competitive intelligence. It can also be useful ammunition in a trade secrets suit. *See, e.g., New England Circuit Sales v. Randall*, No. 1196CV10840, 1996 U.S. Dist. LEXIS 9748 (D. Mass. June 4, 1996), where a key piece of evidence in support of the claim that an Internet marketer was violating his restrictive covenant by working for a new company was the new company's Web site description of its new direction once the employee assumed his new role.

   A company viewing its competitor's Web site should be aware, however, that this practice may not go undetected. Depending on the competitor's tracking software and use of "cookies," it may be possible for the competitor to learn who has visited its site, for how long, how often, and whether they return to the site. Analyzing this information may itself result in valuable competitive intelligence. Therefore, a company considering making a strategic acquisition, for example, might choose to have those investigating the target's Web site use Internet names that are not traceable to the potential acquiring party.
7. *Cf. DoubleClick v. Henderson*, No. 116914/97, 1997 N.Y. Misc. LEXIS 577 (Sup. Ct. N.Y. Co. Nov. 7, 1997), where one defense offered to misusing Internet advertising rate information of their employer was defendants' claim that the employer had posted the same information on its Web site. The court rejected the defense, finding that in fact the employer had posted only generalities, not the specifics at issue. *Cf. EarthWeb v. Schlack*, 71 F. Supp. 2d 299 (S.D.N.Y. 1999), *aff'd in part and remanded in part*, 205 F. 3d 1322 (2d Cir. 2000), holding that certain on-line publishing strategies would not long be secret since they would be revealed by the Web site itself.
8. Information sent by those services remains intact in a mailbox at the service provider which could, in theory, be accessed by the service provider or those who improperly enter the service providers' files, as well as by the intended recipient. Such potential access, however, is not particularly likely. *See* South Carolina Ethics Advisory Opinion 97-08 (June 1997) ("While there exists a potential for communications to be intercepted, albeit illegally, from a commercial network mailbox or an Internet 'router', the Committee does not believe such a potential makes an expectation of privacy unreasonable.").
9. *See Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998) (holding that ECPA criminalizes only the interception of electronic communications contemporaneously with their transmission, not once they have been stored); *Payne v. Norwest Corp.*, 911 F. Supp. 1299, 1303 (D. Mont. 1995) (appropriation of a voicemail or similar stored electronic message does not constitute an "interception" under the statute); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1996); *United States v. Turk*, 526 F.2d 654, 658 n.3 (5th Cir.), *cert. denied*, 429 U.S. 823 (1976). *Cf. United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998) (retrieval of stored voicemail does violate the act).
10. *United States v. Keystone Sanitation Co.*, 903 F. Supp. 803 (M.D. Pa. 1995).
11. *Cf. The T.J. Hooper v. Northern Barge Corp.*, 60 F.2d 737, 740 (2d Cir.), *cert. denied*, 287 U.S. 662 (1932) (L. Hand, J.) (holding that "seaworthiness" is a term whose definition is not fixed but evolves along with technological advances, and concluding that while a seaworthy vessel of an earlier era would not have incorporated a radio, radios were available to vessels of 1928 and thus should have been used). But see the discussion below of various State Bar opinions concluding that failure to encrypt communications with clients is not unethical.

12. Note that, depending on the subject matter, encrypting messages may on occasion trigger the new Export Control provisions.
13. Security measures should be observed on internal "intranets" as well. The touchstone should always be, does the recipient have a business need to see the information? If so, password protection can help ensure that others who have no need to see the information do not see it as well.
14. *United States v. Martin*, Crim. No. 98-CR-48 (D. Me.).
15. Iowa Supreme Court Board of Professional Ethics, Opinion 96-1, 8/29/96. To the same effect, see South Carolina Bar Advisory Opinion 94-27 (Jan. 1995).
16. Opinion 97-1, 9/17/97.
17. *See* South Carolina Bar Ethics Advisory Committee, Opinion 97-08 (June 1997).
18. *See* W. Freivogel, *Communicating with or about Clients on the Internet*, Alas Prevention J., January 1996 and W. Freivogel, *Internet Communications - Part II, A Larger Perspective*, Alas Prevention J., January 1997.
19. *See, e.g.,* Alaska Bar Ass'n Ethics Comm. Op. 98-2 (Jan. 16, 1998) (1998 WL156443), State Bar of Arizona Advisory Ethics Opinion 97-04, 4/7/97, at http://www.azbar.org/ EthicsOpinions; the District of Columbia. Ethics Comm. Op. 281 (Feb. 18, 1998), http://www.dcbar.org/pro-resources/opinions; Illinois State Bar Association Opinion 96-10, 5/16/97; Kentucky Bar Ass'n Ethics Comm. Advisory Op. E-403 (July 1998), http://www.uKy.edu/law/Kyethics; New York State Bar Ass'n Comm. on Professional Ethics Op. 709 (Sept. 16, 1998), http://www.nysba.org/opinions, N.D. State Bar Ass'n Ethics Comm. Op. 97-09 (Sept. 4, 1997) (unpublished); Vermont Bar Association Committee on Professional Responsibility, Opinion 97-5, 13, Law Man. Prof. Conduct 2/0. *See also* ABA Comm. on Ethics & Professional Responsibility Formal Opinion 99-143 (Mar. 10, 1999), www.abanet.org/cpr.; Major Nell, E-mail and Confidential Information, 1999-AUG Army Law. 45 (Aug. 1999).
20. Freivogel, *supra* note 18.
21. *Raytheon v. John Does 1-21*, No. MICV 99-00816F (Mass. Super. Ct., filed Feb. 11, 1999). *See also Pro Med Co Management Co. v. John Does 1-50*, No. 806956 (Orange Co., Calif. Sup. Ct. 1999) (suit brought seeking identity of posters of allegedly defamatory messages which drove down value of plaintiff's stock).
22. Many major ISPs have stated their willingness to provide such identifying information in response to a subpoena, whether with or without notice to the poster. Their specific policies vary. Representative policies regarding how to assert claims of misappropriation of intellectual property may be located at www.lycos.com/ lycosinc/legal.html; http://docs.yahoo.com/mto/terms; http://doc.altavista.com/legal/copyright.shtml.
23. *Ford Motor Company v. Lan*e, 52 U.S.P.Q. 1345 (E.D. Mich. 1999). *See also Sheehan III v. King County*, No. C97-136 OWD (W.D. Wash. 1998), refusing to enjoin a consumer's posting of personal and Social Security information about employees of a credit reporting agency on the Internet on the same grounds.
24. 78 F.3d 219 (6th Cir. 1996).
25. *See Conley v. DSC Communications Corp.*, No. 05-98-01051-CV, 1999 WL89955 (Tex. App. Feb. 24, 1999) (rejecting First Amendment overbreadth challenge to trade secrets injunction since injunction was the only effective way to prevent destruction of the secrets).
26. 28 U.S.C. §§ 1831-1839.
27. *See, e.g., United States v. Riggs*, 743 F. Supp. 556 (N.D. Ill. 1990) (imposing liability under the National Stolen Property Act, 18 U.S.C. § 2314, on two "hackers" who had allegedly stolen files from the telephone company and republished them on the Internet to tell the "hacker" community how to prevent the authorities from discovering their activities. The court held that the transmission "is the very vehicle of the crime itself."). *See also, e.g.*, Cal. Pen. Code § 499C and Cal. Pen. Code § 502 (criminalizing various computer crimes including illegally accessing or copying data).
28. *Cf. Underwater Storage, Inc. v. United States Rubber Co.*, 375 F.2d 950, 955 (D.C. Cir. 1966), *cert. denied*, 386 U.S. 911 (1967) ("Once the secret is out, the rest of the world may well have a right to copy it at will; but this should not protect the misappropriator or his privies.").
29. *See, e.g., Religious Technology Center v. Lerma*, 897 F. Supp. 260, 265 (E.D. Va. 1995) ("Despite [plaintiff's extraordinary efforts to try to maintain' secrecy,] defendant . . . is not the only source of [the documents containing the secrets] on the Internet. Accordingly, for the purposes of this motion, it would seem that plaintiff cannot establish that [the documents] are not 'generally known.'"); *Religious Technology Center v. FactNet, Inc.*, 901 F. Supp. 1519 (D. Colo. 1995) (publication on the Internet destroys trade secrets).
30. 923 F. Supp. 1231, 1255 (N.D. Cal. 1995).
31. *Religious Technology Center v. Netcom On-Line Communication Services, Inc.* (N.D. Cal. Jan. 6, 1997) (emphasis in original).
32. 174 F.3d 411 (4th Cir. 1999).
33. No. CV 786804 (Cal. Super. Ct., Santa Clara Co. Jan. 21, 2000). For the briefs filed in that action, *see* http://www.pzcommunications.com/decss/main.htm.
34. For a list of search engines and their caching policies, *see* http://www.searchenginewatch.com/features.htm.
35. One can foresee a situation in which, to avoid a crushing damages calculation, the initial poster will urge that little harm was actually done by the misdeed and thereby perhaps assume the burden of showing that in fact there was only limited access to the secret. Such a showing might not be binding, however, in subsequent litigation with third parties.
36. *See, e.g.*, Restatement of the Law of Unfair Competition, § 40 (1995).
37. 857 F. Supp. 679 (N.D. Cal. 1994), *modified* 948 F. Supp. 923 (N.D. Cal. 1996).
38. *Religious Technology Center v. Ward* (N.D. Cal. Mar. 21, 1996) (granting temporary restraining order against further solicitation of trade secret materials or publication of secrets).
39. No. 99-CR-174 (E.D.Wisc. 1999).

Victoria A. Cundiff, a partner in the New York office of Paul, Hastings, Janofsky & Walker LLP, is Chair of the Intellectual Property Law Section. She thanks Jennifer Shmulewitz, an associate at the firm, for her research assistance. A version of this article was presented at the Intellectual Property Law Section's Fall Meeting at The Sagamore on October 14, 2000.

ANNOUNCING THE

Intellectual Property Law Section's

ANNUAL LAW STUDENT WRITING CONTEST

Sponsored by THOMSON & THOMSON

To be presented at **The Annual Fall Meeting of the Intellectual Property Law Section, October 11-14, 2001, Lake George, NY** to the authors of the best articles on a subject relating to the protection of intellectual property not published elsewhere.

First Prize: $2,000 Second Prize: $1,000

CONTEST RULES

To be eligible for consideration, the paper must have been written solely by a student or students in full-time attendance at a law school (day or evening) located in New York State or by out-of-state law students who are members of the Section.Papers should be no longer than 35 pages, double-spaced, including footnotes. Submissions must include the submitter's name; law school and expected year of graduation; mailing address; e-mail address; telephone number; and employment information, if applicable. One hard copy of the paper and an electronic copy in Word format on a 3.5 H.D. disk must be submitted by mail, postmarked not later than June 30, 2001, to each of the persons named below. As an alternative to sending the disks, the contestant may e-mail the electronic copies, provided that they are e-mailed before 5:00 p.m. EST, June 30, 2001.

Send entries to:

Walter J. Bayer, II
Co-Chair, Technology Transfer
& Licensing Law Committee
GE Licensing
One Independence Way
Princeton, NJ 08540
(609) 734-9413
(e-mail: walter.bayer@corporate.ge.com)

and:

Victoria A. Cundiff
Chair, Intellectual Property Law Section
Paul, Hastings, Janofsky & Walker, LLP
399 Park Avenue, 30th Floor
New York, NY 10022
(212) 318-6030
(e-mail:vacundiff@phjw.com)

Reasonable expenses will be reimbursed to the author of the winning paper for travel and lodging at the Fall Meeting to receive the Award.

Please direct any questions to Walter Bayer.

2000 Winners

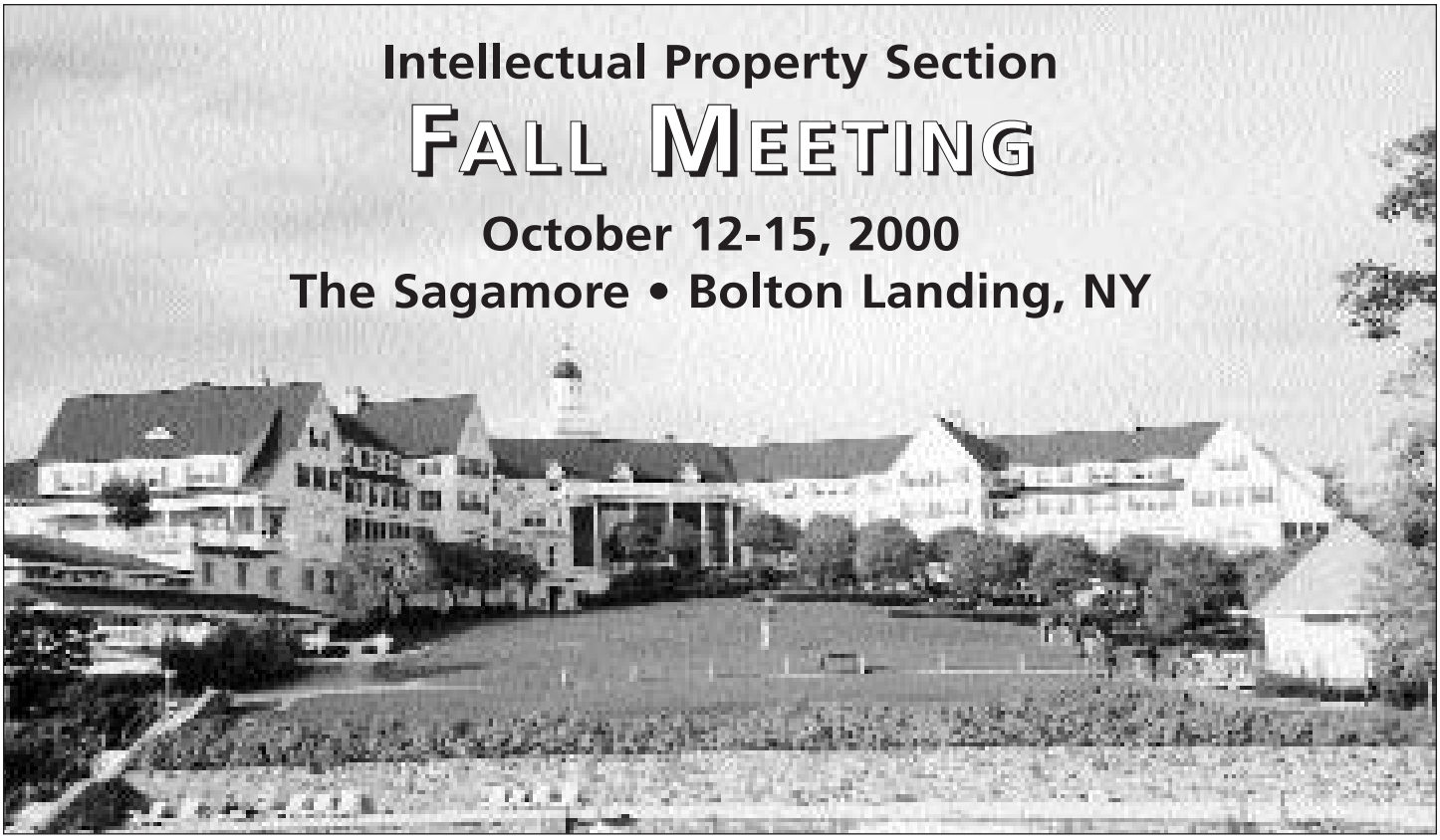
1st Place: **Michael J. Kasdan**
2nd Place: **David R. Johnstone**
Third Place: **Donna Furey**
Honorable Mention: **Darryll Towsley**

The Section reserves the right not to consider any papers submitted late or with incomplete information.

Intellectual Property Section

FALL MEETING

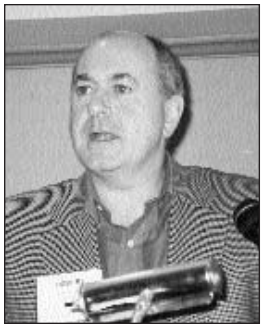
October 12-15, 2000
The Sagamore • Bolton Landing, NY



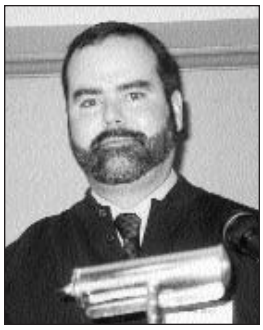






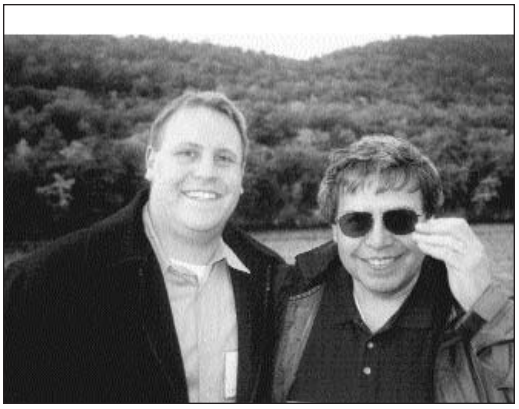



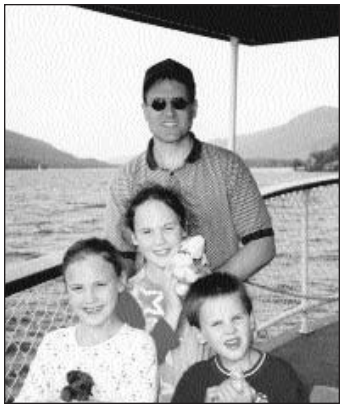


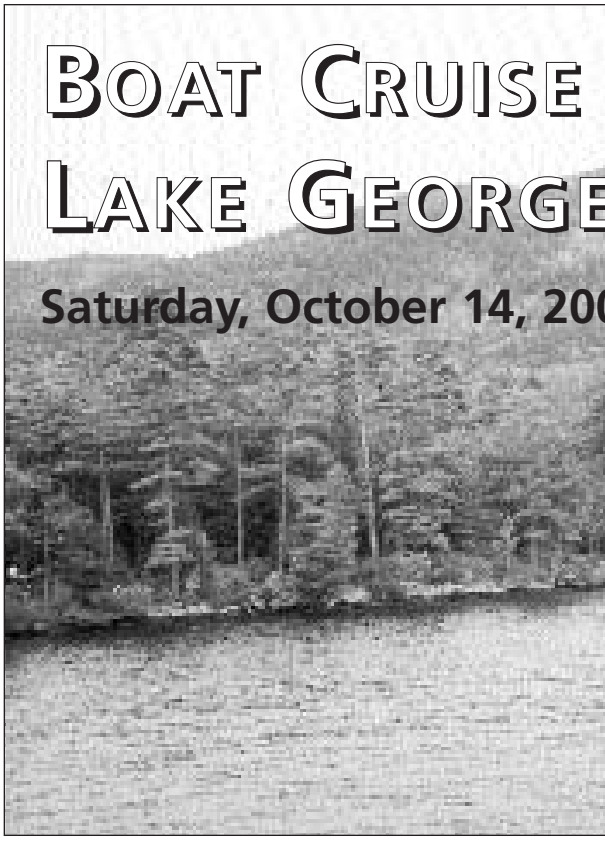


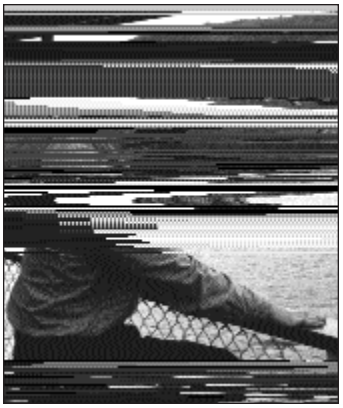


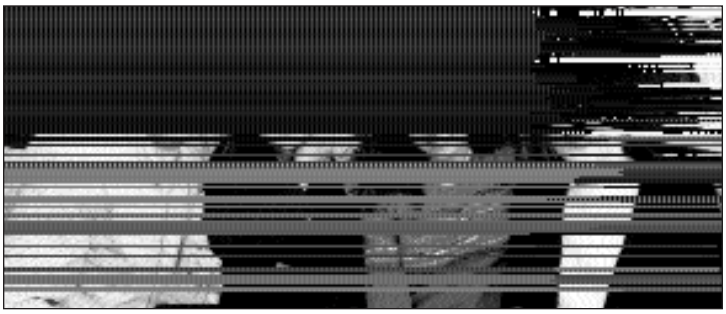


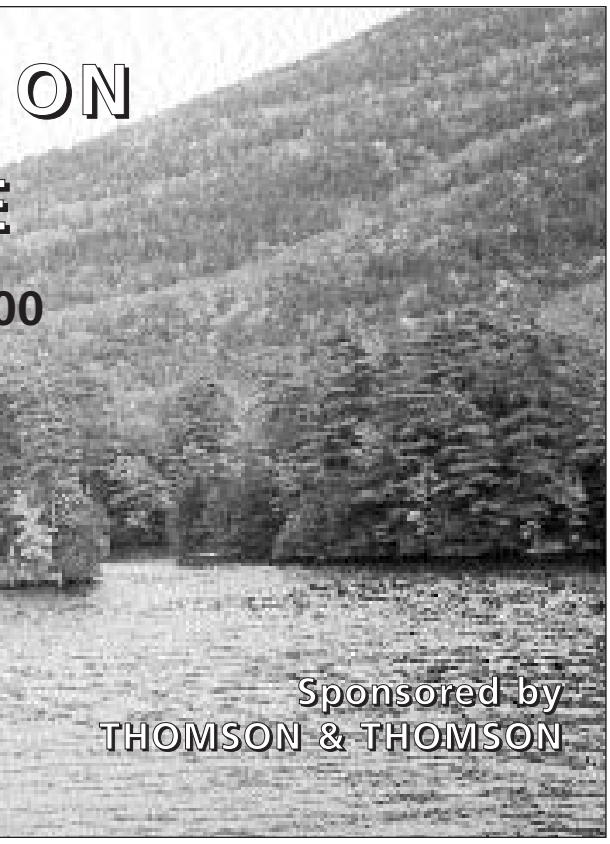



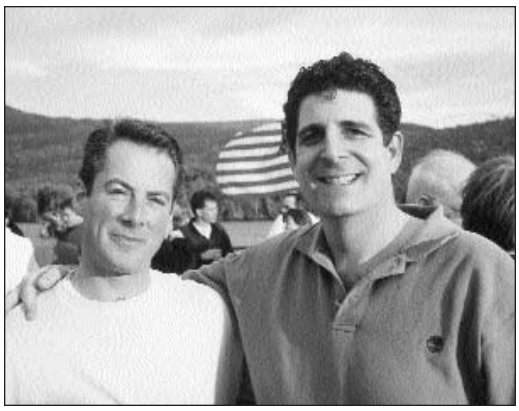


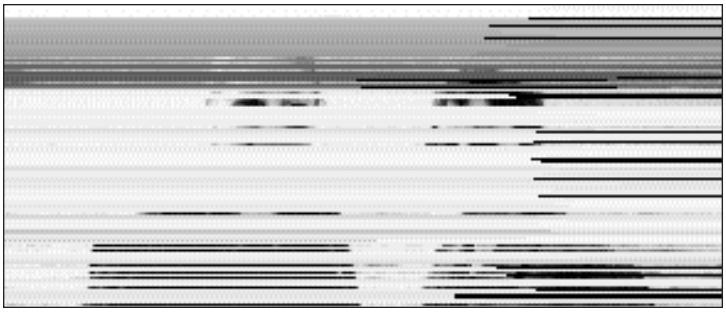

Boat Cruise
Lake George
Saturday, October 14, 200

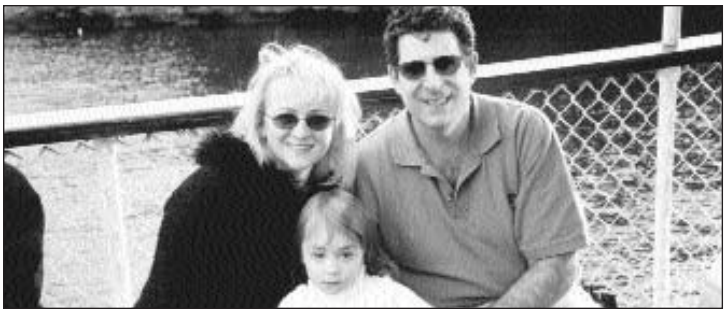





ON
E
00
Sponsored by
THOMSON & THOMSON

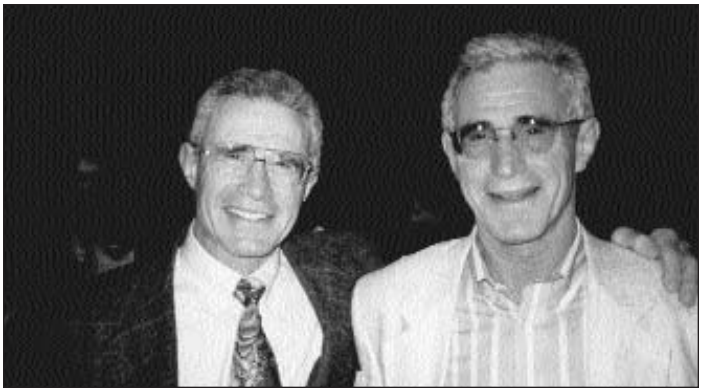







CHILD 4



YOUR PICTURE COULD BE HERE NEXT YEAR!

Intellectual Property Section Meeting

2001 FALL MEETING

October 11-14, 2001

The Sagamore
Bolton Landing, New York

The Section plans to offer a full day of MCLE credits

How Courts Should Do Their Business Regarding Business Methods After *State Street Bank v. Signature Financial Group, Inc.*

By Michael J. Kasdan

I. Introduction

A. A Brave New World of E-Commerce

The exponential growth of the Internet has opened up a networked world of information, has enabled people to better communicate with one another, and has fueled a rocketing New Economy: e-commerce.[1] Examples of this phenomenon abound in contemporary life. Amazon.com's online store has led to a mini-renaissance in book sales.[2] E-Toys delivers millions of Furbies and Pokemon cards to gleeful children each holiday season.[3] eBay has made attics and garages virtual goldmines.[4] Priceline.com allows consumers to name their own price for purchases ranging from groceries to airline tickets.[5] If we feel like some ice cream and a movie but are too lazy to go out shopping, we can hop on the Internet, and Kozmo.com will deliver it to our door by bicycle messenger.[6]

But a potential crisis lurks beneath the surface of this nirvana. As with most new technologies, the development of the Internet has sparked a wrangling for ownership of the New Frontier—battles over who owns the intellectual property that is driving this economic growth engine.[7] A number of potentially broad patents issued by the United States Patent and Trademark Office (PTO) that cover not only narrow technological improvements but basic widespread methods and techniques for doing business on the Internet, are particularly worrisome.[8] For example, Sightsound.com claims to have been granted a patent that covers the entire concept of selling digital audio or video recordings over the Internet;[9] a company called Open Market claims to have several patents that give it exclusive ownership over business-to-consumer e-commerce itself, which makes any company engaged in e-commerce an infringer;[10] DoubleClick, an Internet advertising company, holds a recently issued patent entitled "Method of Delivery, Targeting, and Measuring Advertising Over Networks,"[11] which basically covers the entire workings of the Internet advertising industry.[12]

These business method patents are seen by many as a big problem for competitors and consumers alike.[13] One of the main criticisms of business method patents is that they extend ownership rights over broad concepts and create an unlevel playing field for business itself.[14] While this may be the price we pay to encourage "scientific" innovation, many feel that the market itself already supplies ample incentive for innovations in methods of doing business and that many of these patents are not worth their cost.[15]

B. How Did We Get Here and Where Are We Going?

The U.S. Patent Act, with its constitutional mandate to "Promote Science and the Useful Arts,"[16] requires Patent Law to continually evaluate its relationship and relevance to each new technology. Indeed, since patents were first issued, each revolutionary industry has spawned a new debate over its patentability.[17] A century ago, critics questioned whether agricultural inventions could be protected on the grounds that agriculture was not an industry (a "useful art"). In the 1970s, as pharmaceutical research and development grew, it was argued that granting patents for pharmaceuticals would be unethical. In the last decade, biotechnology was the great new challenge for patent law. The "patenting of life" controversy[18] questioned the ethics of and ability to patent processes and products that are drawn in part from nature. Today, with the rapid explosion of the Internet and e-commerce, the patenting of e-commerce methods and techniques is the latest in what has been an ongoing series of debates regarding what ideas and technological innovations the U.S. patent system can and should protect.

It had long been widely believed that business methods were unpatentable subject matter. However, last summer, in the landmark case *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*,[19] the U.S. Court of Appeals for the Federal Circuit rejected the contention that business methods are not patentable subject matter[20] when it announced that both software and business methods now should be considered patentable subject matter[21] so long as they produce a "useful, concrete, and tangible result."[22] This decision opened the door for multitudes of patents that cover the various methods of transacting e-business, ranging from computerized purchasing methods to online auctions.[23]

While *State Street* has answered the preliminary question of whether business methods are patentable, many unanswered questions remain as to whether or not many of these broad business method patents will be upheld by the courts. This article will explore how the courts should move forward with respect to this new class of patent-eligible subject matter after *State Street*.

With computer-enabled business methods now fair game as patentable subject matter,[24] courts must be increasingly careful as to how they define the scope of these e-commerce patents in infringement actions. Failure properly to construe the limits and bounds of these Internet business method patents will result in a slew of overly broad "bad patents" that will litter cyberspace, muddle the Internet economy,[25] stifle competition in cyberspace, and make the e-commerce arena highly litigious.[26]

In assessing how the patent system should address these e-commerce patents when their validity (aside from subject matter) is challenged, a look to recent history, particularly biotechnology, is instructive. The advent of new technologies has always given the PTO problems; software and the Internet are no different.[27] By tracing the treatment of patents in another controversial cutting-edge area of technology—biotechnology—and then evaluating whether to apply patent doctrine as developed in that area to Internet business methods, this article will attempt to shed some light upon how the patent system can better deal with computer-enabled business method patents.

This article will address the most troubling class of e-commerce patents: hybrids of computer software and business method patents which claim patent protection for computerized systems that implement processes and methods of doing business. To provide a context for a discussion of these patents, Section II traces the historical treatment of both computer software and business methods as patentable subject matter by the courts. Section III examines the impact of *State Street* and summarizes the key legal questions that remain unanswered regarding computerized business method patents. Section IV discusses the statutory requirements of novelty,[28] non-obviousness, and enablement and discusses how these requirements might be used to answer some of the questions left open by *State Street* and to restrict the validity of many broad business method patents. As noted above, the subject matter requirement is only the first door that a potential inventor must pass through on his way to a patentable invention.[29] Because the patent system is based on a societal bargain in which society promotes invention by paying the price of granting the inventor a limited monopoly in exchange for the societal benefit that innovation brings, the requirements of the patent system seek to ensure that each patented invention is truly new, inventive, and given to the public.[30] Thus, to be patentable under the Patent Act, an invention must not only be within the proper subject matter of patentable inventions, but must also be "novel,"[31] "non-obvious,"[32] and adequately disclosed such as to "enable"[33] one who is skilled in the art to make and use the invention.[34] This section will draw parallels as to how the courts have used these statutory requirements to control or expand the reach and scope of patents in infringement actions in biotechnology and have applied these concepts to business method patents. The article concludes that courts performing validity analysis[35] on the hundreds of controversial business method patents should begin to use the novelty, non-obviousness, and enablement sections of the Patent Act[36] to invalidate many business method patents or at least to reduce the scope of many of them.

Finally, in Section V, based upon this comparison, the article applies the heightened legal standards suggested herein to some of today's more controversial business method patents.

II. Historical Treatment of Computerized Business Methods and Software as Patentable Subject Matter

The U.S. Constitution empowers Congress "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writing and Discoveries."[37] United States patent law, as articulated by § 101 of the Patent Act, broadly allows for the patenting of any machine, process, manufacture, or composition of matter that is "new and useful."[38]

The holder of a patent is granted a temporary monopoly over his or her invention in exchange for the inventor's technological contribution to society. The patent system rewards invention by granting an ownership right to the invention, which is realized through the temporary monopoly profits gained from one's invention and protection from infringement under the law during the patent period. This policy encourages innovation and contribution to the technological advancement of society. [39] Patent policy and its statutory requirements are designed to best determine which invention rights are necessarily granted to the patentee in order to optimally motivate innovation and which inventions are better left in the public domain.[40]

Traditionally, courts have held three categories of subject matter to be unpatentable: abstract ideas,[41] phenomena of nature,[42] and the articulation of abstract scientific/intellectual principles.[43] The policy rationale behind these exclusions is rooted in the idea that while one can get a patent on a concrete instantiation of an idea, one simply cannot *own* ideas or scientific princi-

ples and phenomena of nature—these must be left in the public domain as the building blocks of future technological innovation.[44]

It was long thought that techniques such as advances in the social sciences and business management were also excluded subject matter. While such techniques were often useful and pragmatic, they did not address the concrete manipulation of physical forces and were often dismissed as abstract ideas.[45] Recent advances in technology have strained this simplistic understanding, as courts increasingly have been confronted with challenges as to how to apply § 101. Two of the main technological growth areas of the twentieth century, computer software and business methods, have particularly perplexed courts addressing the subject matter requirements of § 101. Computer software programs are really nothing but strings of algorithms, which can be seen as mere ideas that cannot be owned, and hence, cannot be patented. Similarly, courts have had a difficult time distinguishing business methods from abstract ideas.

A. The Early Cases: Software and Business Methods

To fully understand the historical background of e-commerce patents, which generally combine software and business methods, one must look to the historical treatment of patents on software and patents on business methods. Based on the early guidance from Supreme Court precedent, it was long thought that mathematical algorithms/software and business methods fell into the excluded categories.

1. Software

Early Supreme Court case law squarely denied patent protection to software inventions because it required processes to be tied to a physical process. *Gottschalk v. Benson*[46] is a good example of this jurisprudence. The subject matter at issue was a computer program that converted numbers between two binary coded formats. The court held that the patent was invalid on the grounds that it was not statutory subject matter included in § 101, noting that no physical transformation was involved. Similarly, in *Parker v. Flook*[47] the Supreme Court held that a computerized method for updating alarm set-points of a chemical process was not statutory subject matter and hence unpatentable.

In the 1980s however, as software became an increasingly important part of industry and life, patentees began to hone in on the Court's language and attempted to patent software that was tied to some sort of physical process. They recognized that simply by placing a newly discovered mathematical equation within a functional computer program, they could get around much of the precedent excepting abstract mathematics from the subject matter of the Patent Act.[48] In *Diamond v. Diehr*,[49] the court held that a computerized process for curing synthetic rubber, which contained a mathematical algorithm, was patent-eligible subject matter, since it was tied directly to the underlying physical process itself.[50] Again, the fact that computerized elements were applied to a physical transformation was emphasized.[51] *Diehr* was, however, an important turning point, as it allowed for the general patent-eligibility of computer software. The Federal Circuit liberalized and extended the patent-eligibility test for computer software in cases such as *Arrhythmia Research Technology Inc. v. Corazonix Corp*.[52] and *In Re Alappat*.[53] Furthermore, in June 1995, the PTO issued new examination guidelines for evaluating computer-related inventions.[54]

Nonetheless, until *State Street*, the subject matter eligibility of software-related patents remained in doubt because of an unwieldy mechanical test that was used by the Federal Circuit to determine subject matter eligibility in computer software cases. From early cases that focused on the application of computerized method to physical elements, the Federal Circuit created a two-part test, which became known as the Freeman-Walter-Abele test.[55] Under this test, the court (1) inquired whether the patent claims recites a mathematical algorithm, and (2) if a mathematical algorithm is found, whether that algorithm is applied in any manner to physical elements or process steps. If the algorithm is applied in this manner, then the claim is valid § 101 subject matter.

The Federal Circuit did not strictly adhere to this test[56] because, in practice, both steps were difficult to apply. First, it was difficult to define clearly what a "mathematical algorithm" is, within the meaning of the first step. Second, it was difficult to say how much physical activity would satisfy the second step.[57] Thus, on the eve of *State Street*, the law regarding the patent eligibility of computer software inventions was muddled and inconsistent.

2. Business Methods

Early case law also indicated that business plans and business systems were not patent-eligible subject matter under § 101.[58] At the time, this notion seemed to be grounded in good common sense. Earlier this century, it seemed wrong to characterize business methods such as investment management and bookkeeping procedures as innovations in the "useful arts," which are entitled to protection under the patent system.[59] While concrete physical innovations such as motors and oscilloscopes had a clearly protectable technological component, these business methods did not involve any technological component at all.

Early courts that rejected patents under what had come to be called the "business method exception" actually based their opinions on the fact that patent

protection was limited to technology (*i.e.*, tangible things and physical procedures), and the business methods that they were addressing fell below the threshold of this statutory subject matter. However, with the advent of computers, the carrying out of these business methods has migrated from the pen and paper to the code of software programs. Today, it has become much more difficult to categorize software-enabled business methods as "non-technological" and hence not deserving of patent protection.[60] In fact, many of the significant technological innovations in the last decade have come in the area of computer software.[61]

Because the "business method exception" was generally limited to dicta and to the specific facts of the limited technology of early business methods that were being addressed and was not truly developed in holdings, it is impossible to review its historical roots coherently. Nonetheless, a short review of the major cases should help to give context to the impression that a "business method exception" did, in fact, exist.

The case that is often cited as the origin of the business method exception is *Hotel Security Checking v. Lorraine Co.*,[62] which involved a patent for a bookkeeping method. There, the court found that a "method and means for cash-registering and account checking" which was designed to monitor the honesty of employees, was not eligible subject matter because it was an abstraction rather than an art.[63] However, because the court had already found that the invention at issue was not patentable due to lack of novelty, the court's statement regarding business methods is only dictum.[64] Nonetheless, until 1996 the PTO's Manual of Patent Examining Procedure (MPEP) contained a provision codifying the "business method exception" which cited to *Hotel Security Checking*.[65] Moreover, many leading treatises recognized the existence of a "business method exception."[66]

In many other cases throughout the century, business method patent claims were often rejected as falling outside of the realm of statutory subject matter. Naturally, some of these claims were rejected on an alternative ground of lack of novelty, non-obviousness, or failure of enablement. Thus, although there were a few exceptions,[67] many cases rejecting business method patents cited to *Hotel Security Checking* and the "business method exception."[68]

In light of *State Street*, one transitional case that is of interest is *Paine, Webber, Jackson, & Curtis Inc. v. Merrill Lynch*.[69] There, the court validated a business method patent that covered a service method of combining a margin brokerage account with money market funds and a checking/charge account. *Paine, Webber* held that "a business system may be patentable in the form of a suitably programmed computer system."[70] The *Paine, Webber* court was not focused on the general patent eligibility of business methods, but on the patentable use of a computer in the system. This case can be attributed to the modern recognition, sparked by the combination of business methods and computer systems, that business methods can no longer be classified as non-technological subject matter that is per se non-deserving of a patent. It can be seen as an interesting precursor to *State Street*'s unequivocal rejection of the business method exception.

B. *State Street*: The Shift for Software and Business Methods

The patent at issue in *State Street*[71] was Signature Financial Group's now famous (or infamous) '056 patent, entitled "Data Processing System for Hub and Spoke Financial Services Configuration."[72] The patent disclosed a computerized business system that allows the assets of two or more mutual funds to be pooled into another investment portfolio that is organized as a partnership.[73] It claimed that the usefulness of this system was that it facilitated quick and accurate calculation of each mutual fund's valuation.

The Massachusetts district court applied the Freeman-Walter-Abele[74] test and held that the '056 patent was invalid under 35 U.S.C. §101 as claiming an unpatentable mathematical algorithm.[75] The Federal Circuit, however, reversed and articulated a more liberal and expansive test for the patent-eligibility of software claims that incorporate algorithms, holding that as long as it produces "a useful, concrete, and tangible result," such subject matter is eligible for patent protection.[76] The *State Street* court also took the opportunity to "[lay the] ill-conceived [business method] exception to rest,"[77] noting that business methods are subject to the same statutorily defined legal requirements for patentability as any other process or method.[78] Thus, *State Street* had two extremely significant holdings with respect to patentable subject matter. The first was that software is patentable subject matter. The second was that business methods are patentable subject matter.

State Street is thus credited with opening up two classes of subject matter that had previously been considered closed off from the patent system: software and business methods. [79] Naturally, this has introduced some complexities in how these new subject matter patents are to be dealt with.[80]

III. The Impact of *State Street*: Some Questions Resolved, Others Left Unanswered

A. The Impact of *State Street*

In our burgeoning Internet economy, *State Street* has provided e-commerce companies with a method of protecting their Internet business method ideas that many had previously considered unpatentable. The *State*

State Street decision has opened the door to the protections of the patent system for the emerging e-commerce industry, and has also exposed industries that had previously been outside the realm of patent protection and infringement issues, such as the financial services industry.[81] This opening up of the availability of patent protection to business methods as subject matter is reflected in the large increase in the number of business method patent applications that the Patent and Trademark Office has received over the past year.[82] Inventors have recently gained patent monopolies over such subject matter as a method of aggregating mutual funds into larger pools,[83] the reverse Dutch auction method of selling product,[84] distributing audio and video file over the Internet,[85] giving online users rewards for clicking on ads,[86] real-time payment using credit and debit cards over the Internet,[87] and using "electronic shopping carts" to track purchases over the Internet.[88] They plan to use these broad monopolies to crush their competition by excluding them.[89]

To say that many of these patents are highly controversial is a vast understatement.[90] Critics fear that *State Street* and the ensuing issuance of broad patents that cover methods of conducting business on the Internet will have a negative effect on both the economics of cyberspace and competition between online businesses.[91] Many feel that allowing individual entities to control broadly defined central methods of doing business will preclude robust competition and wreak havoc on the level playing field of the business world's landscape.[92] As noted by one author who is chronicling the emerging patent battles between e-commerce players in high-tech fields, "You're not patenting a better mousetrap; you're giving out ownership rights over the idea of trapping mice."[93] Moreover, many assert that if the business landscape of the Internet consists of minefields of hundreds or thousands of patents covering many computerized ways of doing business, it will be harder to assemble them to actually *do* business in an economy that moves at Internet speed.[94] Critics further question the ability of the Patent Office to determine what is novel and non-obvious (and hence worthy of patent protection) when deciding whether or not to grant patents in the fast changing environment of cyberspace.[95]

B. Key Post-*State Street* Questions

Today, the critical question regarding many of these Internet business method patents is whether they are valid. Each day a growing number of high-profile patent infringement actions are filed, pitting e-commerce players against each other in the early battles for Internet dominance.[96] These cases will test the limits of how well many of these the business method patents will stand up in court. While *State Street* has been accepted as law on the question of subject matter,[97] the larger question of whether courts will uphold many of these controversial patents as valid still remains unanswered.[98]

While many of these criticisms are worthy, they do not mean that *State Street*, which was limited to allowing software and business methods as patentable subject matter, was wrong. Rather, the historical evolution of the treatment of both business methods and computer software[99] show us that *State Street*'s determination that computer software and business methods, and hence computer-enabled business methods, are patent-eligible subject matter was not surprising.

It is important to remember, however, that the *State Street* holding does not mean that all Internet business method patents are valid—only that business methods as a class are *eligible* for patent protection. Although business methods, as a general class, now constitute patentable subject matter within the meaning of § 101, the secondary question of whether each particular business method patent in question satisfies the other substantive requirements of the Patent Act must be determined on a case-by-case basis. As the Federal Circuit stated in *State Street*: "Patentability does not turn on whether the claimed method does "business" instead of something else, but on whether the method, viewed as a whole, meets the requirements of patentability as set forth in Sections 102 [Novelty], 103 [Non-obviousness], and 112 [Enablement] of the Patent Act."[100]

Thus, while *State Street* expanded the scope of eligible subject matter, it merely shifted the central validity inquiry away from subject matter[101] to novelty, utility, non-obviousness, and enablement. The novelty and non-obviousness requirements ensure that the subject matter is indeed new and innovative and is not apparent, given the state of the art. The enablement requirement seeks to distinguish an idea from the embodiment of an idea by requiring that the inventor actually allow the public to benefit by adequately disclosing the details of the invention.[102] Only future litigation challenging the scope of business method patents will help shape the standards to be applied to patent claims involving this new subject matter and determine the role that these Internet business method patents will play in e-commerce.[103]

Two of the main functions of these statutory requirements—restricting the ownership of ideas themselves and controlling the broad scope of patents—squarely address the central concerns of many of *State Street*'s critics. Applying these requirements to the subject matter of Internet business methods is the challenge to courts in the post-*State Street* era. It is the job of the courts to learn to apply these requirements to Internet business methods in such a way that individual entities do not end up owning an overly broad exclusive

monopoly over "the idea of trapping mice" that would restrict innovation and fly in the face of the policies behind the patent system.

IV. Dealing With the New Subject Matter: How Far Do We Go?

In determining which patents are valid and which are invalid under the statutory standards, courts must keep in mind the central policy aims of the patent system. Just as they must when evaluating the patentability of any new subject matter or technology, courts examining business method patents must consider which policy goals are desirable and construe patent doctrines to achieve them.

A. The Parallel Acceptance of Biotechnology and Computer Software as Patentable Subject Matter

When dealing with any new technology, there is always a transitional period during which inventions that may seem obvious to experts in that field are granted patent rights. This effect is illustrated by both biotechnology and Internet business method patents.[104]

Since *State Street* was decided in 1998, there have been few court decisions addressing Internet business patents.[105] However, biotechnology is another controversial technology whose key patentability issues were decided only relatively recently. Biotechnology patents presented a similar problem because courts had to decide how close a line to draw between nature and invention. There were concerns that a principle of nature, just like a mathematical algorithm or a scientific principle, should not be protected by a patent. Therefore, in order to evaluate the appropriateness of Internet business method patents, it will be instructive for courts to look at how this issue was addressed in the biotechnology area.[106]

The broadening of the law of subject matter in the business method software arena that was started in *Diamond v. Diehr*[107] and completed in *State Street*[108] mirrors the shift in biotechnology towards patent-eligibility of that subject matter in the landmark Supreme Court case *Diamond v. Chakrabarty*.[109] In fact, *State Street* applies the same principles to business methods as *Chakrabarty*[110] did for biotechnology: while almost every subject may be eligible for patent protection, not everything is patentable.

In *Chakrabarty*,[111] the Supreme Court noted that "anything under the sun that is made by man" is patentable.[112] Due to the combination of many groundbreaking advances in biotechnology, with this expansive reading of the subject matter requirement[113] many patents involving biotechnological subject matter became the subject of infringement litigation. While patentees asserted infringement, defendants challenged the validity of this new class of patents. To resolve these disputes, courts had to decide how far to extend patent protection over the new subject matter. Several Federal Circuit opinions dealing with biotechnology show an interesting consideration of how the statutory requirements of novelty, non-obviousness, and enablement requirements should be applied to the new subject matter. These approaches are laid out below and compared to the approach that this article suggests should be taken with business method patents.

B. Restricting the New Subject Matter: A Comparison and a Proposal

1. Novelty and Non-Obviousness

The bedrock principle of patent law is that in order to receive a patent you must invent something new.[114] This simple idea is codified in 35 U.S.C. § 102, the novelty provision of the Patent Act, which requires a determination as to whether each element of the invention is found in a single piece of prior art. This provision lists the types of prior art that can cause a patent not to be granted. Each type of prior art can establish that the invention has already been invented by another, and, hence, that the patentee should not be granted a patent. A further, less technical, requirement is that patents should be granted only for inventions that are non-obvious over the prior art. Non-obviousness has often been called the "ultimate condition of patentability"[115] because it attempts to measure an even more abstract quality than novelty. While the novelty requirement is limited to whether each element of the invention is captured in one piece of prior art, the function of the non-obviousness requirement[116] is to determine whether the invention, albeit novel, is a sufficient technical advance over the state of the art to be deserving of a patent.[117] As stated by the Supreme Court: "Innovation, advancement, and things which add to the sum of useful knowledge are inherent requisites in a patent system which by constitutional command must 'promote the Progress of . . . useful Arts.'"[118] The non-obviousness requirement is the prime enforcer of that constitutional command.[119]

The modern test for non-obviousness requires a flexible analysis of multiple pieces of prior art and an inquiry as to whether "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the art to which the subject matter pertains."[120] This determination has been cast by the Supreme Court into a three-part factual inquiry followed by a determination of law.[121] First, the court must determine the scope and content of the prior art. Second, the court must determine how the patentee's invention is different from the prior art. Third, the court must determine who is the ordinary skilled worker in

the art. After this three-part inquiry, the court must apply the statutory standard and determine whether the invention as a whole would have been obvious in light of the prior art at the time of invention to an ordinary worker of skill in the art.[122] In making this determination, courts should focus on how hard it was to find the solution to the problem, and whether the prior art contained "suggestions or motivations to make the invention." Courts may also consider certain "secondary considerations" as objective indicia of non-obviousness such as the commercial success of the invention, acquiescence in the marketplace (taking of licenses), previous failure of others to make the invention, and long-felt yet unfulfilled need for the invention.

New technologies pose special problems for a clear application of both the novelty and obviousness inquiries. These problems are both practical and theoretical. On a practical level, in new areas of technology, there is often a dearth of prior art with which to compare the invention.[123] On a more theoretical level, however, the PTO and the courts must determine whether an application of a new technology to an old method of doing something is novel or obvious.

Moreover, it is clear that the obviousness inquiry is highly technology-dependent.[124] In newer, more unpredictable arts such as biotechnology, the non-obviousness requirement will be easier to satisfy than in more mature predictable arts such as the mechanical, electrical, or chemical arts, where theories are better known. As evidenced by many of the central biotechnology cases, which construe the obviousness requirement as only a very patent-friendly "easy" standard, and affirm the validity of many patents, this results in the issuance of many patents within these new technologies.[125]

In *In re Deuel*,[126] the Federal Circuit held that despite the existence of prior art references which taught the method of gene cloning from a partial amino acid sequence and a reference that disclosed the partial amino acid sequence of a protein, the patent on cloning the cDNA for that specific protein was nonetheless non-obvious. In order to find obviousness, the court required not only that the prior art references be structurally similar to the claimed compound, but that they clearly suggest the invention. The existence of a well-known general method for isolating cDNA molecules was considered irrelevant.[127] Similarly, in *In re Bell*, the Federal Circuit reversed the PTO's original finding of obviousness for a patent claiming human gene sequences which code for insulin-like growth factors. There, although the PTO examiner found that the patent was obvious due to the presence of prior art which disclosed the amino acid sequences for the insulin-like growth factors and a prior art reference which disclosed a method of cloning genes from amino acid sequences, the Federal Circuit reversed, finding that because no prior art suggested using the method for these specific amino acids that "the requisite teaching or suggestion to combine the teachings of the prior art references is absent."[128] It seemed to many in the biotechnology field, however, that with access to the known DNA library structure and the method of probing, the patented sequences could be determined by merely following known steps and therefore were not inventive. Indeed, most reasonably skilled biotechnologists thought that the leap from amino acids to proteins was very shallow indeed, and were shocked that the court held these to be non-obvious.

It is clear from the discussion thus far that the non-obviousness inquiry has been applied by the PTO to both biotechnology and business method patents in a very similar fashion; that is to say, it has been largely ignored, or at least quite diluted. It is important however, to draw principled conclusions from the biotechnology jurisprudence.

Commentators have suggested that the biotechnology jurisprudence discussed above illustrates the court's willingness to interpret the non-obviousness doctrine in a manner that supports their policy goals.[129] Robert Merges has suggested that the Federal Circuit intentionally used this patent-friendly standard of obviousness to preserve the important, yet fledgling patent-dependent biotechnology industry. Biotechnology is an industry where, although much of the research and development is "obvious" from a legal standpoint, that research and development is highly intensive and would be prohibitively expensive without the possibility of patent protection.[130] In this manner, some envision the courts manipulating the obviousness requirements in certain industries in order to arrive at a desired policy result of increasing the ease or difficulty of obtaining patents.

Other commentators have noted, however, that it is wrong for courts to apply such a low standard of obviousness. They complain that "the Federal Circuit has effectively tilted the balance far in favor of biotech patent applicants through its definition of the legal test of what constitutes a proper prima facie case of legal obviousness,"[131] and advocate the adoption of a less stringent requirement for "suggestion" from the prior art and a higher standard of inventiveness in the obviousness inquiry.[132]

Regardless of whether it is right or wrong for the courts to make it easier to attain patent rights in industries such as biotechnology, it is important to consider whether their obviousness standards (or lack thereof) should be blindly applied to business methods. It is apparent from the issuance of the hundreds of controversial business method patents noted above[133] that the PTO has adopted a very similar patent-friendly test for non-obviousness in the business method sphere as well.

The biotechnology cases illustrate that the courts have wide discretion in their application of the nonobviousness doctrine. The same need for patents to protect an important and nascent industry that may have driven the court's application of a lower obviousness standard in biotechnology simply does not exist in the business method arena. While the existence of business method patents has allowed some aggressive companies to secure broad rights and build businesses around those rights,[134] the viability of e-commerce is not based around ability to secure these patent rights. In order to survive in the business world, companies must continually compete through innovations in their business methods and the services that they offer to customers, and they will be amply rewarded for these efforts by the market. Moreover, the cost of research and development for the invention of Internet business methods is quite minimal, as opposed to the substantial cost, time, and experimentation required to develop biotechnology innovations and reduce them to commercially viable products. Clearly, the lower obviousness standard applied in the biotechnology patents is not appropriate for business method patents.

A more rigorous obviousness doctrine that only grants patents for true inventions will ensure that the patent system will be used as a tool for innovation, and not as a blockade against it.[135] Courts must ensure that the policy standards that underlie the patent system are being served by the PTO. This requires courts to raise the non-obviousness bar in the business method arena.[136] This means that business method patents for inventions that are either non-novel or non-obvious should be struck down as invalid. The crucial step that courts must take in this regard lies in the first part of the traditional obviousness inquiry: determining what is contained in the prior art.[137] Many of today's most controversial patents involve old public domain ideas that have simply been ported to the Internet and applied to a computer context. In the art of software development, for example, the inventive step taken by a skilled programmer to computer-enable a previously known business method may in most cases be completely obvious. The key doctrinal step that must be taken in the non-obviousness inquiry is to stop falsely separating cyberspace from "real" space.[138] Courts must consider traditional business methods as part of the set of prior art that informs e-commerce business methods.[139] Courts could even go a step further by holding that Internet business methods based on existing business methods are prima facie obvious.[140] This places the burden on patentees to show what they have added, modified, and invented. It is reasonable that some of the truly innovative business method patents will and should stand up to this higher level of scrutiny.

While this modification will not automatically invalidate all Internet business method patents, by allowing the traditional business methods to act as prior art, the courts will at least force patentees into showing that they have added some inventive step such that the invention as a whole would not have been obvious at the time of invention in light of the prior art to an ordinary worker of skill in the art.[141] Correct application of this non-obviousness standard will lead to the necessary closer scrutiny of many of today's most controversial Internet business method patents. For example, if traditional Dutch auctions were considered prior art against Priceline's reverse Dutch auction patent, and the traditional business method of "putting something on your tab" were considered prior art to Amazon.com's "one-click" patent, courts could then at least begin to conduct a true non-obviousness inquiry.

2. Enablement

A second powerful mechanism for controlling the scope of patents that should be utilized when assessing the validity of business method patents[142] is the enablement requirement.[143] The policy rationale underlying the enablement requirement is two-fold: Firstly, it ensures that the inventor truly discloses the invention to the public.[144] Secondly, it acts to control the scope of the patented claims by narrowing the coverage of the claims to only those parts that are adequately disclosed.

Rather than restricting the domain of patentable inventions, as the obviousness requirement does, the statutory enablement provision restricts the scope of the patent claims. Simply stated, enablement requires that the inventor describe the invention sufficiently in the patent disclosure so that a person skilled in the art can understand it well enough to make it and use it, without undue experimentation. If the description is so vague or uncertain that no one can determine, except by undue experimentation, how to make or use the patented device or process, then the patent is void. This effectively prevents patentees from claiming overly broad interpretations of their patent's claims in infringement actions, and acts as a mechanism of distinguishing unpatentable ideas from potentially patentable embodiments of ideas.

The famous *O'Reilly v. Morse*[145] decision is the paradigm of how enablement is meant to distinguish between ideas and embodiments of ideas in tangible products. There, the Supreme Court invalidated Morse's broadest telegraph patent claim, claim 8, which claimed the use of electromagnetism "however developed, for marking or printing intelligible characters, signs, or letters, at any distances." The Court noted that claim 8 was invalid because it purported to encompass products or processes that the specification of the patent did not sufficiently teach the public to make and use.[146] The Court's decision in *Morse* may be understood as ruling that at too great a level of abstraction, a patent claim is no longer understood as directed to a

specific embodiment, but to an idea.[147] Morse simply sought to claim a patent monopoly over more than he invented.

Commentators have noted that one of the reasons why business method patents are perceived as so troubling is the difficulty in resolving their apparently broad scope.[148] While for ordinary machines and processes, patent law has been quite successful in distinguishing between unprotectable abstract ideas and protectable physical embodiments of ideas, in both business methods and computer-implemented inventions there has been more of a "difficulty of properly titrating scope of protection to enabling disclosure."[149] This is perhaps best illustrated by the history of software patents,[150] throughout which the Federal Circuit often struggled with how to regard the use of computer algorithms in patents.

This problem, however, is not insurmountable. Moreover, as illustrated by the example above, "ambitious" over-inclusive claiming is not a problem unique to software-enabled business methods. As PTO Commissioner Q. Todd Dickinson noted in responding to the many criticisms of Internet business method patents, the U.S. patent system has worked for centuries and will continue to work effectively to spur innovation.[151] He reasons that many of these seemingly broad Internet broad business methods should be and will be narrowly construed by the courts in infringement actions. Holding patentees to a more exacting standard of enablement will decrease the number of patents whose claims are absurdly broad and purport to capture entire principles or ideas instead of narrow instantiations of innovative ideas.[152] For example, enablement should block patentees who attempt to extend their claim construction to cover virtually any commerce transacted over the Internet,[153] while allowing narrower claims which properly cover instantiations of ideas relating to e-commerce.

Again, lessons may be extracted from a comparison to biotechnology patent jurisprudence. For arts such as biotechnology, while the obviousness requirement will be easier to satisfy due to the unpredictable nature of the art,[154] the enablement requirement will be more difficult to satisfy for precisely the same reason. Because the technology is often unpredictable and sometimes difficult to recreate, the biotechnology enablement jurisprudence requires quite exacting narrow claiming to fully enable one skilled in the art to make or use the invention without undue experimentation.[155] Thus, while the relatively relaxed non-obviousness standard leads to the issuance of many patents in unpredictable arts such as biotechnology, their scope and vitality are unknown and potentially quite narrow due to an exacting enablement standard.[156]

By way of comparison, in arts such as software or business methods, which are not as unpredictable and hence easier to properly disclose and enable, it would seem to follow that the frequency of rejections due to non-enabling disclosures should be quite low. However, this will not necessarily be the case for many of these controversial patents. Although it is facially easier to properly fulfill the enablement requirement, courts must not disregard the enablement requirement; instead, they still must give careful scrutiny to abusive overly broad claiming practices that have been used in many of the most controversial Internet business method patents.[157] As illustrated by the Morse patent, overly broad claiming can occur in any patent regardless of the underlying technology. In order to effectively police the scope of these patents, the more exacting enablement jurisprudence which we are used to seeing applied to technologies such as biotechnology also should be applied to Internet business methods to demand and enforce narrower claiming.

V. Application to Today's Business Method Patents

Many of the Internet business method patents that have been referred to throughout this article are particularly troubling both because of the apparent obviousness of their claimed "invention" and because of the breadth of their claims. This section will briefly illustrate how the two-pronged application of both the heightened obviousness and stricter enablement standards suggested by this article could be used to invalidate or narrow the scope of many of these controversial patents.

Two of the better known Internet business method patents, Amazon.com's vaunted "1-click" patent[158] and Priceline.com's famed reverse Dutch auction patent[159] each claims broad rights over seemingly obvious and fundamental known methods simply by porting these methods to the Internet/computer context. For example, Amazon's '411 patent covering its "1-click" technology essentially claims the right to the business method of storing user information and using such stored information to facilitate the quick and easy purchasing of products from a Web site. Specifically, the process claimed in the '411 patent comprises the steps of (1) allowing an online buyer to send a purchase request along with an identifier of the buyer to the seller; (2) the seller site receiving the request and using the identifier to retrieve previously stored additional information about the buyer (such as his or her credit card information and mailing address); and (3) generating a purchase order for the buyer using the retrieved information about the buyer. Similarly, Priceline.com's '127 patent, upon which its entire Web site (indeed, its entire corporate existence) is based, claims a method compromising: (1) entering a purchase offer which includes an

offer price, accompanied by the buyer's credit card number; (2) sending the offer to the seller; (3) entering an acceptance of the highest offer by the seller; and (4) paying the seller using the buyer's submitted credit card number.

Amazon's 1-click patent simply claims the concept of a user account or "tab," where customer information, such as a credit card number or mailing address is kept from previous purchases and applied to new sales. Priceline's '207 patent, like Amazon's '411 patent, simply adds the step of using a personal computer and the Internet to the well-known method practicing reverse auctions. Neither seems inventive enough to merit patent protection. Under the heightened obviousness standards suggested in Part IV.B.1 above, because both reverse auctions and user accounts are long-standing traditional business methods that have been used for many years, Amazon and Priceline should either have to overcome a prima facie case of obviousness, or, in the alternative, affirmatively prove that in light of prior art, which includes traditional business methods, their method is non-obvious.

Additionally, if the stricter standard of enabling disclosure suggested above were applied by the Federal Circuit, the scope of many of these patents, even if they are found non-obvious, could be significantly narrowed. Just as Morse's patent sought to claim rights to any use of electromagnetism for transmission of information, many Internet business method patents seek to claim coverage of downloads of digital data over the Internet,[160] auctions over the Internet,[161] or storing and using user information in conjunction with any sales over the Internet.[162] Many of these claims are ludicrously broad, and should be struck down.

While this would not be a complete solution because future patent attorneys would more carefully tailor their claims and enabling disclosures, application of this standard would be helpful in two ways. First, it will act as a deterrent to the overall practice of aggressively overbroad claiming. Second, it will weaken the scope of many of the existing Internet business method patents that are embroiled in industry-wide litigation.[163] As the PTO grows and adapts to the new subject matter that it must consider by adding software and business experts, by gathering larger sets of relevant prior art, and by initiating uniform policies and standard operating procedures which control how such subject matter is addressed, future Internet business method patents should not be as problematic as today's Internet business methods.[164]

While such scrutiny of patent validity may seem unlikely in light of the Federal Circuit's extreme deference to the PTO and the strong presumption of validity given to issued patents,[165] it is important for the Federal Circuit to reestablish proper standards in this area of patent law. Given the magnitude of the problems that could be caused by excessively widespread issuance of broad Internet business method patents,[166] the Federal Circuit must now act affirmatively to address the patents that have issued in the wake of *State Street*.[167] Once the PTO acquires greater sophistication in addressing patent applications for Internet business method patents, greater deference to the validity of patents will again be proper.[168]

VI. Conclusion

Applying a low non-obviousness bar and minimal enablement requirement to Internet business method subject matter has wrongly awarded patent grants to non-innovative contributions. This resultant "over-patenting" of obvious ideas has led to a spate of infringement actions asserting broad, non-novel, and obvious business method patents which read onto basic processes used by scores of e-commerce to conduct their everyday business. In contrast, in the biotechnology area, the application of an extremely patent-friendly non-obviousness doctrine, along with a strict enablement doctrine has resulted in what commentators, who question whether such patents are worth having at all, have termed a "tragedy of the anticommons":[169] a splintering of rights, where many small rights provide their holders with little benefit, but still must be maneuvered around to do business and to innovate.

By applying the two-pronged approach of both a heightened obviousness and heightened enablement standard to this new subject matter, the Federal Circuit can avoid the equally troubling scenarios of the over-patenting of obvious subject matter associated with the current state of Internet business method patents, and the splintering of rights associated with the current state of biotechnology patents. This approach will ensure that patent law as applied to Internet business methods works no differently than the policy goals motivating the patent system compel it to work in all other areas of patentable subject matter: patent protection should only be granted to concrete instantiations of truly innovative ideas.

Endnotes

1. *See generally* Daniel Amor, The E-Business Revolution 1 (2000) (exploring e-commerce and noting that "[o]ver the last few years the Internet has evolved from being a scientific network only, to a platform that is enabling a new generation of businesses. The first wave of electronic business was fundamentally the exchange of information. But, with time, more and more types of businesses have become available electronically. Nowadays we can buy goods online, book holidays or have texts translated over the Internet in an instant."); Carl Shapiro and Hal Varian, Information Rules (1999).

2. *See* Time's 1999 Person of the Year at http://www.time.com/time/poy/intro.html (visited May 22, 2000) (Amazon.com CEO Jeff Bezos is named 1999's Person of the Year for his pioneering launch of Amazon.com, the largest Internet seller of books in the world).

3. *See* E-Toys Homepage at http://www.e-toys.com (visited April 15, 2000).

4. *See* eBay at http://www.ebay.com (visited April 15, 2000).

5. *See* Priceline.com at http://www.priceline.com (visited April 15, 2000).

6. *See* Kozmo.com, at http://www.kozmo.com (visited April 15, 2000).

7. *See* Richard Poynder, *Method Madness: The Battle Over E-Commerce Heats Up*, IP Magazine, Nov. 1999, available at http://www.ipmag.com/monthly/99-nov/methodmadness.html (visited May 22, 2000) (detailing the newest controversial "patenting wrangle," which involves patents covering e-commerce methods and techniques). *See also* Rodney Ho, *Patents Hit Record in '98 as Tech Firms Rushed to Protect Intellectual Property*, Wall St. J., Jan. 15, 1999, at A2 (noting the record numbers of issued patents, many of which purport to cover Internet processes).

8. An addition complication is that patent applications are maintained in secrecy until they are granted. As a result, patents filed two or three years ago in the formative stages of the Web are only now being granted. When many of these broad patents issue, they cover what most of the industry is already doing, making everybody an infringer who must pay royalties. *See* Saul Hansell, *Surging Patents*, N.Y. Times, Dec. 11, 1999, at C1.

9. *See* U.S. Patent No. 5,966,440, filed on June 12, 1997, issued on November 9, 1999; *See generally* Richard Poynder, *A Patently Damaging Firefight*, Financial Times, May 12, 1999, at B4 (chronicling Sightsound's patent infringement suit against online music vendor, N2K/CDNow.com and noting that Sightsound has demanded royalties in every online sale of digital music from companies such as MP3.com, Goodnoise, and Amplified.com).

10. They include a patent on secure real time credit-card payment, a patent on electronic shopping carts, and another patent on analyzing how users browse Web content. *See* Seth Schulman, *Software Patents Tangle the Web*, Technology Review, March/April 2000, at 70.

11. *See* U.S. Patent No. 5,948,061, filed on Oct. 29, 1996, and issued on September 7, 1999.

12. *See* Chris Oakes, *Patents New Result: Nothing?*, Wired News, at http://www.wired.com/news/tech/0,001,595,45000,00.html (Sept. 13, 1999) (discussing DoubleClick's far reaching business method patent on advertising over the Internet as an example of yet another "futile Internet patent").

13. As a spokesperson for BarnesandNoble.com said in addressing their dispute with Amazon.com over a key business method patent: "We do not intend to sit back and allow Amazon to stake a claim upon any technology that is widely used. Allowing them to do so abridges our rights as a leader in e-commerce, but more importantly limits the choices of consumers."

14. *See generally* James Gleick, *Patently Absurd*, N.Y. Times Magazine, Mar. 12, 2000, at 44-49 (chronicling the Amazon "1-click" patent and concluding that applying patents to thoughts and ideas in cyberspace could kill e-commerce).

15. *See, e.g.*, Lawrence Lessig, *The Problem with Patents*, The Industry Standard, Apr. 23, 1999, available at http://www.thestandard.com/article/display/0,1151,4296,00.html (visited May 22, 2000) (arguing that "just because some [patent] protection is good, doesn't mean that more is better," concluding that the only result of such unbounded intellectual property protection will be the production of more lawyers: "Only one thing is certain about more and stronger IP: It will produce more lawyers. That's great for me, producer of lawyers that I am. But what's great for the likes of me is not necessarily great for cyberspace").

16. U.S. Const., § 8 cl. 8.

17. *See* Poynder, *supra* note 7 (documenting the history of patentability struggles of each new technological subject matter).

18. *See generally* Robert Cook-Deegan, Gene Wars: Science, Politics, and Human Genome (1999); Universal Declaration of the Human Genome and Human Rights, at http://www.unesco.org/ibc/uk/genome/projet/index.html (visited May 22, 2000) (an example of bio-ethical issues raised by the human genome project, and attempts to patent "life.")

19. 149 F.3d 1368 (Fed. Cir. 1998).

20. "As an alternative ground for invalidating the '056 patent under § 101, the court relied on the judicially-created, so-called 'business method' exception to statutory subject matter. We take this opportunity to lay this ill-conceived exception to rest. Since its inception, the 'business method' exception has merely represented the application of some general, but no longer applicable legal principle, perhaps arising out of the 'requirement for invention'—which was eliminated by section 103." *State Street*, 149 F.3d at 1375.

21. The *State Street* decision had two separate aspects: the first confirmed the patent-eligibility of computer software, while the second announced the patent-eligibility of business methods. This article will address the highly controversial computerized business methods that lie at the intersection of the two parts of the court's analysis: software and business methods.

22. *State Street*, 149 F.3d at 1373.

23. *See* Greg Aharonian, *1998 Software Patent Statistics*, Internet Patent News Service, Nov. 1998 (on file with author) (noting that over 17,500 software patents were issued in 1998, along with 300 Internet patents, and 700 financial/business patents); Schulman, *supra* note 10 at 68 (noting that the PTO is now receiving over 2500 applications per year for "business method software patents").

24. *State Street* allows all business methods (not only computer enabled business methods) to be eligible subject matter for a patent. This article, however, will focus on computer-enabled business methods (patents that combine software with a business method), as they are the most prevalent and controversial patents today.

25. *See* Poynder, *supra* note 7 (In e-commerce the cost of paying licensing fees for each technique used in a transaction becomes prohibitively expensive. "You may have to use compression technologies, watermarking technologies, encryption technologies, clearinghouse technologies—all of which could be an essential component of a digital distribution system. . . . Paying royalties on all these technologies adds up, and represents a very significant cost factor.")

26. *See* Lessig, *supra* note 15 ("'Bad patents' thus become the space debris of cyberspace. Nowhere is this clearer than in the context of business-method patents. At a recent conference in Israel, I watched as a lawyer terrified the assembled crowd of Internet startups with stories of the increasing number of business-method patents that now haunt Internet space. Patent No. 5,715,314, for example, gives the holder a monopoly over 'network-based sales systems'—we call that e-commerce. Patent No. 5,797,127 forms the basis for Priceline.com and effectively blocks any competitor. Patent No. 4,949,257 covers the purchase of software over a network.")

27. *See* Schulman, *supra* note 10 at 74 ("Taking a long historical view, much of the current patent conundrum stems from the advent of a new and uncharted technological realm. The Patent Office has almost always had problems with dramatic technology shifts, and software and the Internet are not exceptions.").

28. PTO Commissioner Q. Todd Dickinson, in addressing concerns over the negative impact of a slew of broad e-commerce business method patents, has said "that is not going to happen because if they have been used for years, and publicly, then a patent cannot be issued, as the method is not novel." Poynder, *supra* note 7.

29. *See State Street*, 149 F.3d at 1372 n.2 (*citing In re Bergy*, 569 F.2d 952, 960, 201 USPQ 352, 360 (CCPA 1979) (emphases and footnote omitted)):

> The first door which must be opened on the difficult path to patentability is § 101. . . . The person approaching that door is an inventor, whether his invention is patentable or not. . . . Being an inventor or having an invention, however, is no guarantee of opening even the first door. What kind of an invention or discovery is it? In dealing with the question of kind, as distinguished from the qualitative conditions which make the invention patentable, § 101 is broad and general; its language is: "any * * * process, machine, manufacture, or composition of matter, or any * * * improvement thereof." Section 100(b) further expands "process" to include "art or method, and * * * a new use of a known process, machine, manufacture, composition of matter, or material." If the invention, as the inventor defines it in his claims (pursuant to § 112, second paragraph), falls into any one of the named categories, he is allowed to pass through to the second door, which is § 102; "novelty and loss of right to patent" is the sign on it. Notwithstanding the words "new and useful" in § 101, the invention is not examined under that statute for novelty because that is not the statutory scheme of things or the long-established administrative practice.

30. Martin Adelman, et al., Cases and Materials on Patent Law 1 (1998) ("at essence the patent system offers the inventor a relatively simple bargain: disclosure of a technological advance in exchange for the right to exclude others from employing it.").

31. 35 U.S.C. § 102.

32. 35 U.S.C. § 103.

33. 35 U.S.C. § 112.

34. Rebecca Lynn Eisenberg, *Amazon's Patents Hurt Technology,* available at http://www.cbsmarketwatch.com/news/current/rebecca.htx (Mar. 15, 2000) (noting that in order to qualify for a patent, the invention must be novel, non-obvious, and useful to the public: "These requirements were necessary to preserve a delicate balance—if too few patents were issued, then inventors would be left without protection. But if too many patents were issued, inventions would be claimed and controlled by parties who had not created them, to the detriment of individuals and companies that need them to further innovation.").

35. In patent litigation courts must determine both if the patent is valid (validity analysis) and if it is infringed (infringement analysis). Each of these phases gives courts some leverage to categorically shrink the breadth and scope of patents. It should be noted that despite the proposals of this paper, a finding of patent invalidity has become increasingly rare in recent years. *See In re Zurko*, 142 F.3d 1447 (Fed. Cir. 1998) (en banc) (establishing strong presumption of validity). *See also Markman v. Westview Instruments*, 517 U.S. 370 (1996) (claim construction is to be construed using intrinsic evidence such as the patent itself, the file history, and the prior art considered by the examiner and not extrinsic evidence). Methods of infringement analysis such as use of a less broad doctrine of equivalents and insisting on a strict "all elements" rule could also control the scope of business method patents. That discussion, however, is outside the scope of this article.

36. *See* Title 35 of the United States Code.

37. U.S. Const., § 8 cl. 8.

38. "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101.

39. Adelman, *supra* note 30, at 1-2.

40. *Id*.

41. *See Fuller v. Yentzer*, 94 U.S. 288 (1877); *Burr v. Duryee*, 68 U.S. 531 (1864).

42. *See Funk Brothers Seed Co. v. Kalo Inoculant Co.*, 333 U.S. 127 (1948).

43. "Phenomena of nature, though just discovered, mental processes, and abstract intellectual concepts/ideas are not patentable, as they are the basic tools of scientific and technological work." *Gottshalk v. Benson*, 409 U.S. 63 (1972). Thus the mere articulation of a scientific principle is excluded, while the implementation of that principle in a functional way may be patented.

44. Hence no one could patent (and hence be able to exclude others from using) the Pythagorean theorem or electromagnetic theory.

45. As a matter of fact, the district court in *State Street* held that the defendant's accounting system patent was unenforceable since it was an abstract idea regardless of whether it was a business system or a mathematical algorithm. The Federal Circuit later overruled this holding. *See State Street Bank and Trust Co. v. Signature Financial Group, Inc.*, 927 F. Supp. 502 (D. Mass 1996), *rev'd*, 149 F.3d 1368 (Fed. Cir. 1998). *See generally* Adelman, *supra* note 30, at 83 (explaining basic concepts of patent eligibility).

46. 409 U.S. 63 (1972).

47. 437 U.S. 584 (1978).

48. *See id*. at 105 (explaining evolution of patent law regarding software).

49. 450 U.S. 175 (1981).

50. The *Diamond* court noted that it did not view the patent claims of the computerized method of curing rubber "as an attempt to patent a mathematical formula, but rather to be drawn to an industrial process for the molding of rubber products." *Diamond*, 450 U.S. at 192-93.

51. "[W]hen a claim containing a mathematical formula implements or applies that formula in a structure or process, which, when considered as a whole, is performing a function which the patent laws were designed to protect (e.g., transforming or reducing an article to a different state or thing), then the claim satisfies the requirements of § 101." *Diamond*, 450 U.S. at 192.

52. 958 F. 2d 1053 (Fed. Cir. 1992). *Arrythmia Research* upheld the validity of an invention that was the practical application of an abstract idea. The invention processed electrocardiograph (EKG) signals from patients heartbeats through a series of calculations, and the final result, output information for heart activity, was the useful, concrete, or tangible thing that represented the patient's heart condition.

53. 33 F.3d 1526 (Fed. Cir. 1994). *In re Alappat* involved a mathematical algorithm that transformed data from an electrical input signal to produce a smooth waveform display on a monitor. The court held that the calculations constituted a practical application of the abstract underlying idea because the smooth waveform on the monitor constituted a "useful, concrete, and tangible result." *In re Alappat*, 33 F.3d 1526, 1544 (Fed. Cir. 1994).

54. *See* Adelman, *supra* note 30, at 147 (quoting from the Patent, Trademark, and Copyright Journal article describing the new guidelines for the examination of computer-related inventions).

55. This test was derived from three decisions of the precursor court to the Federal Circuit, the Court of Customs and Patent Appeals: *In re Freeman*, 573 F.2d 1237 (CCPA 1978); *In re Walter*, 618 F.2d 758 (CCPA 1980); and *In re Abele*, 684 F.2d 902 (CCPA 1992).

56. *See generally* Donald S. Chisum, *Background on State Street Bank and the Patentability of Machine-Implemented Business Methods* 1-22 (Mar. 10, 1999 Santa Clara) (on file with author).

57. *See, e.g., In re Schraeder*, 22 F.3d 290 (Fed. Cir. 1994) (claim to a competitive bidding method not patentable because a mathematical algorithm is implicit in the claim and mere data gathering with no display step is not sufficient "physical activity"); *In re Warmerdam*, 33 F.3d 1354 (Fed. Cir. 1994) (claim to method for generating data structure, by locating a medial axis, to be used in controlling a robot comprises "unpatentable manipulation of ideas" and does not require physical activity); *Arrythmia Research Technology v. Corazonix Corp.*, 958 F.2d 1053 (Fed. Cir. 1992) (patent claiming human heart EKG signal analysis methods is patentable because "output is not an abstract number but is a signal related to a patient's heart activity); *In re Iwahashi*, 888 F.2d 1370 (Fed. Cir. 1989) (claim to voice pattern recognition system is properly claimed as an apparatus with a hardware element of ROM); *In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994) (en banc) (means applying mathematical algorithm to convert waveform data into waveform display on oscilloscope is patentable subject matter because algorithm is applied to physical process).

58. This became known as the "business methods exception." *See Hotel Security Checking v. Lorraine Co.*, 160 F. 467 (2d Cir. 1908).

59. *See* Robert C. Sheinfeld and Parker H. Bagley, *Virtually Anything is Patentable*, Symposium: IP Rights in Methods of Doing Business, Mar. 25, 1999, at 2 (on file with author).

60. *See id*. (noting how difficult it is to draw the proper line between technological and non-technological now that business methods and physical devices are being embodied in computers).

61. *See generally* Simpson L. Garfinkel, Architects of an Information Society (1999) (chronicling the development of the Internet, the Web, Ethernet, time-shared computers, UNIX, RSA encryption, the X Windows system, and many other technologies).

62. 160 F. 467 (2d Cir. 1908).

63. "A system of transacting business disconnected from the means of carrying out the system is not, within the most liberal interpretation an art. Advice is not patentable." *See Hotel Security Checking*, 160 F. at 469.

64. "If at the time of Hick's application there had been no system of bookkeeping of any kind in restaurants, we would be confronted with the question whether a new and useful system of cash-registering and account-checking is such an art as is patentable under the statute. . . . The question seems never to have been decided by a controlling authority and its decision is not now necessary." *Hotel Security Checking*, 160 F. at 472.

65. "Though seemingly within the category of process or method, a method of doing business *can be rejected as not being within the statutory classes*. *See Hotel Security Checking*, 160 F. 467 (2d Cir. 1908), and *In re Wait*, 24 U.S.P.Q. 88, 22 C.C.P.A. 822 (1934)." Manual of Patent Examining Procedure § 706.03(a) (Aug. 1993) (emphasis added).

66. *See* Donald S. Chisum, 1 Chisum on Patents § 1.03[5] and § 1.02[4](1998); P.D. Rosenberg, Patent Law Fundamentals § 6.02[3][b] (2d ed. 1997).

67. *See Rand McNally & Co. v. Exchange Scrip-Book Co.*, 187 F. 984 (7th Cir. 1911) (coupon book of travel units held patentable); *Cincinnati Traction Co. v. Pope*, 210 F. 43 (6th Cir. 1913) (coupon book of detachable parts held patentable).

68. *See In re Wait*, 73 F.2d 982 (C.C.P.A. 1934) (holding that process of communicating terms of contract and recording acceptance of those terms unpatentable); *In re Sterling*, 70 F.2d 910 (CCPA 1934) (holding unpatentable "an ingenious and convenient" method of transferring funds); *Loew's Drive-In Theaters Inc. v. Park-In Theaters*, 174 F.2d 547 (1st Cir. 1949) (holding unpatentable a scheme for parking automobiles in an open lot); *In re Schrader*, 22 F.3d 290 (Fed. Cir. 1994) (holding unpatentable a patent for the method of competitive bidding on many items). *But see In re Schrader*, 22 F.3d 290 (Fed. Cir. 1994) (Newman, J. dissenting) (criticizing business method exception to patentability and stating "since it is . . . an unwarranted encumbrance to the definition of statutory subject matter in section 101, my guidance is that it be discarded as error-prone, redundant, and obsolete").

    Note that *State Street* reversed all of the prior cases that had held the business methods are unpatentable subject matter, including *Hotel Security Checking*. Under *State Street*, all business methods, whether computer enabled or not, should be and should have always been considered patentable. For further discussion of *State Street*, *see infra* Part II.B.

69. 546 F. Supp. 1358 (D. Del. 1983).

70. Chisum, *supra* note 56, at 5.

71. *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F.3d 1368 (Fed. Cir. 1998).

72. *See* Signature Financial's U.S. Patent No. 5,193,056, filed March 11, 1991, and issued on March 9, 1993, entitled "Data processing system for hub and spoke financial services configuration."

73. This "Hub-and-Spoke" arrangement was used to gain various tax and administrative advantages.

74. *See supra* notes 55-57 and accompanying text for discussion of this test.

75. Alternatively, the lower court found that it was invalid due to the business method exception. *See State Street Bank and Trust Co. v. Signature Financial Group, Inc.*, 927 F. Supp. 502 (D. Mass 1996), *rev'd*, 149 F.3d 1368 (Fed. Cir. 1998)

76. *State Street*, 149 F.3d at 1375. The new test is basically practical utility, without regard to whether the useful result is expressed in numbers such as profit, price, etc.

77. *Id.*

78. Note that in § 101, "processes" are one of the enumerated subject matters covered by the patent system.

79. An in-depth discussion of pure business method patents or pure software patents is beyond the scope of this article.

80. Examples of some of the early efforts to deal with new subject matter are business method prior user rights and Amazon's proposal for shortened (five-year) term for these patents. *See, e.g.*, Scott Hillis, *Amazon Wrestling with Patent Case Calls for Reform*, at http://www.yahoo.com/news/amazon_patent.html (visited March 9, 2000). This article, however, focuses on judicial determinations and not potential legislation.

81. *See* Donald S. Chisum, *The Supreme Court and Patent Law, Does Shallow Reasoning Lead to Thin Law*?, 3 Marq. Intell. Prop. L. Rev. 1, 19 (1999) (noting as example that the Priceline.com Internet airline purchase system has raised tens and hundreds of millions of dollars for a system of doing a business that would be worthless if not covered by an enforceable patent); *See also* Matt Richtel, *Are Patents Good or Bad for Business Online?*, N.Y. Times, Aug. 28, 1998, at C1.

82. The PTO granted 1,390 Internet-related patents in the first half of 1999, compared to only 648 in all of 1997. *See* Hansell, *supra* note 8.

83. *See* Signature Financial's U.S. Patent No. 5,193,056, filed March 11, 1991, issued March 9, 1993.

84. *See* Priceline Patent 5,794,207, filed September 4, 1996, issued August 11, 1998; *See generally Priceline.com May Be Next Internet Rocket*, Wall St. J., Feb. 19, 1999 (describing centrality of computerized reverse-auction patent to Priceline.com's business and potential legal troubles)

85. *See* Sightsound.com Patent No. 5,966,440, filed on June 12, 1997, issued November 9, 1999.

86. *See* Netcentives Patent No. 5,774,870, filed on December 14, 1995, issued June 20, 1998.

87. *See* OpenMarket Patent No. 5,715,314, filed on October 24, 1994, issued February 3, 1998.

88. *See id.*

89. *See, e.g., Amazon.com v. BarnesandNoble.com*, 73 F. Supp. 2d 1228 (W.D. Wash. 1999) (granting preliminary injunction against BarnesandNoble.com's use of the "1-click" business method on its e-commerce book site); Tatiana Boncompagni, *Double Trouble*, at http://www.lawnewsnetwork.com/stories/A14311-2000Jan26.html (visited January 27, 2000) (discussing the details of the *DoubleClick v. L90 Inc.* lawsuit).

90. This is evidenced by the growing number of law review articles about *State Street*. *See also Online: A Flood of Web Patents Stirs Dispute Over Tactics*, Wall St. J., Oct. 9, 1998 (discussing many of the traditional business methods that are being patented by "creating an online parallel for a familiar concept in the real world," using frequent flier miles as an example to contrast American Airlines and Netcentives); Dugie Standeford, *Book Publisher Launches Cyber Campaign Against Amazon.com*, E-Commerce Law Weekly, Mar. 8, 2000 ("In a Feb. 28 open, online letter, Tim O'Reilly of O'Reilly & Associates warned Amazon.com chief Jeff Bezos that one-click ordering is not new and that continuing efforts to enforce the over-broad patent 'serve only to hold back further innovation':

> We believe that the rapid innovation on the World Wide Web and Internet platform that has created so much new value for the public (as well as for Amazon and its shareholders) will be choked off if companies take the short-sighted route of filing patents on commonly accepted and obvious techniques in an attempt to keep competitors from using them,

O'Reilly wrote."); Schulman, *supra* note 10 at 76 ("it might behoove us to all park our electronic shopping carts for a moment and try to remember what the patent system is all about—and what it's not.").

91. Brenda Sandburg, *Madness In PTO's E-Commerce Method: It Doesn't Take a Genius To Try Out Old Ideas on the Net But it Can Win You a Patent*, IP Magazine, available at http://www.ipmag.com (Aug. 27, 1998) ("Building on a month-old federal appeals court decision, the U.S. Patent and Trademark Office has recently issued a stream of potentially broad patents covering methods for conducting business on the Internet. The latest patents are significant because they are among the first to explicitly detail Internet applications—and because they involve business practices that have been around for years in the off-line world. Although their final scope ultimately rests with the courts, they are considered to include the most viable and sweeping claims to date."); *See also* Richtel, *supra* note 81.

92. *See* Oakes, *supra* note 12 (quoting Tim O'Reilly's open letter to Amazon.com); Leo J. Riskind, *The State Street Bank Decision: The Bad Business of Unlimited Patent Protection for Methods of Doing Business* (forthcoming 2000, on file with author) (arguing that the economic analysis of patent protection does not support the extension of protection to methods of doing business); *See generally* Gleick, *supra* note 14, at 44-49 (chronicling the Amazon "1-click" patent and concluding that applying patents to thoughts and ideas in cyberspace could kill e-commerce. Gleick notes that "the digital revolution worked without patents. The great bursts of technological innovation of the past two decades, the rise of personal-computer software and the spread of the Internet, took place in a freewheeling and competitive climate, with ideas bouncing at light speed from one place to another." *See* Eisenberg, *supra* note (noting that the inability of the PTO to keep up combined with bad court rulings has led to "a long stream of not-just-bad-but-downright-awful patents on obvious and common processes and methods, placing control in the hands of big companies that can and are using the patents to squelch innovation and progress—the very things that patent law was designed to foster").

93. *See* Boncompagni, *supra* note 89; *See also* Gleick, *supra* note 14, at 48 (quoting Lawrence Lessig, who notes that "We're not talking about Thomas Edison inventing the light bulb. . . . We're not talking about Monsanto spending tons of money on some chemical whatever. We're talking about people taking ways of doing business and, because they put it into software, they say, 'This is now mine.'").

94. *See* Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 Science 698, May 1, 1998 (chronicling the "tragedy of the anticommons," which refers to the under-use of a resource that results from diffuse ownership of inter-related property rights. In the context of the Internet, this could occur if various underlying patent rights needed to create further innovation are held by many different entities. Due to the high costs of bargaining and the heterogeneous interests of the various owners, this fragmented patent rights could lead to under-development of important innovations.). S*ee also* Gleick, *supra* note 14, at 49 (noting that "the digital revolution worked without patents. The great bursts of technological innovation of the past two decades, the rise of personal-computer software and the spread of the Internet, took place in a freewheeling and competitive climate, with ideas bouncing at light speed from one place to another.")

95. Critics of these e-commerce business method patents are troubled by these patents for several reasons: (1) hampering of competition: if companies are able to obtain patents for their business models, it could preclude potential competitors from getting into the game; (2) a handful of lucky and innovative companies could end up owning patents on very basic business models that could be applied to many types of businesses; (3) something is only considered patentable if it is "novel," is not too obvious, and has some kind of usefulness. Since the online world is so new and changes so quickly, the patent office has no way to gauge how innovative these business models really are and whether they merit patents. While the office could do so reasonably well for manufacturing economy, critics question its ability to do so in the new information economy. *See* Richtel, *supra* note 81. *See also* Aharonian, *supra* note 23 (criticizing the PTO's inability to prosecute business method software patents); Jennifer Sullivan, *Net Overloads US Patent Agency*, Wired News, available at http://www.wired.com (May 4, 1999) (critics fear the PTO—despite its key role in the information age—just doesn't "get" the Internet); Sandburg, *supra* note 91 (noting that most Internet business method patent are obvious, as they only are applying old processes to the Internet).

96. Two of the most high-profile of this class of lawsuits are the recent *Amazon.com Inc. v. BarnesandNoble.com Inc.*, No. C99-1695 (W.D. Wash. Dec. 1, 1999) suit regarding one-click technology and *Priceline.com v. MSFT* suit involving Priceline's reverse Dutch auction method.

97. *Court Declines to Review Ruling Seen as Software Boon*, N.Y. Times, Jan. 12, 1999, at B2 (reporting that the U.S. Supreme Court denied the cert. petition in *State Street*). While many academics at first debated the merits and disadvantages of allowing business methods to be patentable subject matter, the Supreme Court denied cert. The Federal Circuit *State Street* opinion is now the law of the land and a discussion of the wisdom of the

decision has become somewhat moot. It is widely considered to be an improvement over the nebulous and difficult to understand tests that it has replaced.

98. In fact, *State Street* purposefully left these questions open to be tested in later cases. The only question at issue in *State Street* was whether the patent passed the subject matter requirement of the Patent Act. While the court found that it did, the opinion noted, "The plain and unambiguous meaning of section 101 is that any invention falling within one of the four stated categories of statutory subject matter may be patented, provided it meets the other requirements for patentability set forth in Title 35, i.e., those found in sections 102, 103, and 112, ¶2." *State Street*, 149 F.3d at 1372.

99. *See supra* Part II (discussing historical treatment of software and business methods).

100. 149 F.3d at 1375 n.10 (*quoting In re Schrader*, 22 F.3d 290, 298 (Fed. Cir. 1994) (Newman, J. dissenting)).

101. 35 U.S.C. § 101.

102. One famous example of how enablement can restrict an overly broad claim is the patent applications of Bell and Morse for their break-through telephone and telegraph inventions. Morse's claim read: "I do not propose to limit myself to the specific machinery . . . described in the foregoing specification, the essence of my invention being the use of motor power of . . . electromagnetism however developed for marking or printing intelligible characters . . . at any distances." Similarly, Bell's claim read: "The method of, and apparatus for, transmitting vocal or other sounds telegraphically . . . by causing electrical undulations." Bell's patent was upheld as valid, while Morse's was struck down held invalid. One way to read this is to say that Morse's was so broad that it sought to claim the actual principal of nature itself, while Bell claimed a useful instantiation of the principle. The enablement requirement can be used to control this by requiring that the claim sufficiently enables the reader to make and use the patent. Describing a detailed technological invention enables, while trying to claim too much by claiming a principle does not.

103. Future legislation could also accomplish such standard-setting, but this article will focus only on standard setting through litigation partially because this author believes that is the better approach. Legislation will still have to be interpreted by the Federal Circuit and has the potential to be misinterpreted. Further, court decisions and standard setting by the Federal Circuit will be of more guidance to the PTO when evaluating patent applications, than mere legislation. The role given to the Federal Circuit by Congress was to better unify patent law between the states and between courts and the PTO; it is the body with the most expertise regarding patent policy and has the ability to effect change.

104. For example, when the PTO allowed patents on DNA sequences, many in the industry felt that this granted patent rights over the mere application of widely known processes.

105. Although many suits have only recently been filed and are pending. *See, e.g.*, *Priceline.com v. Microsoft*.

106. *See* Jared Earl Grusd, *Internet Business Methods: What Role Does and Should Patent Law Play?*, 4 Va. J.L. & Tech 9 (1999) (also suggesting courts look to biotechnology because they "provide a good illustration of courts' willingness to manipulate established doctrine to achieve desired policy outcomes").

107. *See* Diehr, 450 U.S. at 182 ("courts 'should not read into the patent laws limitations and conditions which the legislature has not expressed'") (citation omitted).

108. In fact, the *State Street* court noted explicitly that after the Supreme Court decisions in *Diehr* and *Chakrabarty*, the Freeman-Walter-Abele test had no applicability to determining whether a claim is statutorily acceptable subject matter. *State Street*, 149 F.3d at 1373.

109. 447 U.S. 303 (1980).

110. *Id*.

111. *Id*.

112. *Id.* at 309. This reflects the policy judgment that subject matter should not constrain patentability as long as the patent is a man-made invention and not a mere idea, nature, or abstract principles. These should remain free of ownership, as they are the building blocks of innovation. *See supra* Part II.

113. Older opinions suggested that biotechnology was not patentable subject matter because it was nature. *See Funk Bros. Seed Co. v. Kalo Inoculant Co.*, 333 U.S. 127, 130 (1948).

114. *See* Robert P. Merges, Patent Law and Policy: Cases and Materials 221 (2d ed. 1997).

115. Nonobviousness—The Ultimate Condition of Patentability (J. Witherspoon, ed., 1980).

116. *See* 35 U.S.C. § 103.

117. *See* Merges, *supra* note 114, at 479 ("The theory is that even if an invention is new and useful, it does not deserve a patent if it represents merely a trivial step forward in the art. This is why non-obviousness is the final gatekeeper of the patent system.").

118. *Graham v. John Deere Co*., 383 U.S. 1, 2 (1966).

119. Because the non-obviousness inquiry encompasses the novelty inquiry, in that it considers combining multiple prior art reference, these provisions will be discussed together. Generally, because novelty requires every element of the invention to be present in a single reference, and the non-obviousness inquiry more flexibly allows combining references to determine if an invention would have been obvious, the non-obviousness inquiry is the tougher hurdle and will be focused on in this article.

120. 35 U.S.C. § 103(a).

121. *See* the famed Supreme Court "trilogy" of *Graham v. John Deere Co.*, 383 U.S. 1 (1966), *Calmar Inc. v. Cook Chemical Co.*, 383 U.S. 1 (1966), and *United States v. Adams*, 383 U.S. 39 (1966).

122. Judge Rich has pictured this as the average artisan sitting in his shop, with the prior art posted on the walls all around him. *See In re Winslow*, 365 F.2d 1017 (CCPA 1966) (describing the "Winslow tableau"). It has been acknowledged, however, that this conception is somewhat misleading because the very point of the obviousness inquiry is to determine whether it would be evident to one of ordinary skill to select the particular references that exist all over the world and combine them.

123. These practical timing problems will tend to solve themselves over time. As the PTO gets more and more prior art over time, examiners ultimately learn the contours of the new field in a better way. *See* Teresa Riordan, *Historians Take a Longer View of Net Battles*, N.Y. Times, Apr. 10, 2000, at C1 (noting that our history of innovations and of the PTO being confronted with new technologies, including the telegraph, telephone, radio, and television, illustrates that "the lag between the skills of the patent office and innovation has been there for a long time," and more importantly that it is too early to tell how innovative new inventions within a technology are until the "dust [has] settle[d]").

124. Many commentators have suggested that different applications of obviousness to different technologies reflect a different conception of the role of patents in different industries. *See, e.g.,* Richard R. Nelson, The Sources of Income Growth (1996) (suggesting that patents are very important in pharmaceuticals and chemical industries, but are less important in the mechanical and electrical fields); John Kasdan, *Obviousness and New Technologies*, 10 Fordham I. P., Media & Ent. L.J. 159, 184 (1999) (concluding that the patent system is not very important in software and that business methods are more like that field than any other; thus, obviousness standards should be adjusted to reflect that). *See also* Merges, *supra* note 114, at 603 (discussing biotechnology).

125. *See, e.g.*, *In re Bell*, 991 F.2d 781 (Fed. Cir. 1993); *In re Deuel*, 51 F.3d 1552 (Fed. Cir. 1995); *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367 (Fed. Cir. 1986).

126. *In re Deuel*, 51 F.3d 1552 (Fed. Cir. 1995).

127. *See id*. at 1559 ("The PTO's focus on known methods for potentially isolating the claimed DNA molecules is also misplaced because the claims define compounds, not methods. . . . [T]he existence of a general method of isolating cDNA or DNA is essentially irrelevant to the question of whether the specific molecules would have been obvious.").

128. *In re Bell*, 991 F.2d at 785.

129. *See* Merges, *supra* note 114; Grusd, *supra* note 106, at ¶ 70 (noting that "[t]he biotechnology cases illustrate that courts have discretion in their interpretation of the nonobviousness doctrine").

130. *See* Merges, *supra* note 114, at 600-01 ([F]or the time being the court has preserved the possibility of patent rights in this important branch of industry. Perhaps if this branch continues to be valuable, a decision that raises the standard of patentability here will cause problems for the industry. One suggestion is to give a slight "plus" factor to obvious but very expensive research.").

131. Anita Varma & David Abraham, *DNA is Different: Legal Obviousness and the Balance Between Biotech Inventors and the Market*, 9 Harv. J.L. & Tech 53, 55 (1996).

132. They would advocate a strict standard for what is invented as in *Fiers v. Sugano*, 984 F.2d 1164, 1206 (Fed. Cir. 1993), rather than the patent-friendly standard for what is nonobvious applied in *In re Deuel*, 51 F.3d 1552 (Fed. Cir. 1995).

133. *See supra* notes 8-12 and 82-89 and accompanying text.

134. *See, e.g.*, Walker Digital's Priceline.com, at http://www.priceline.com.

135. *See* Heller & Eisenberg, *supra* note 94 (detailing the detrimental effects of a patent system that fails to strike the proper balance in their granting of patents).

136. *See* Grusd, *supra* note 106, at ¶ 70 ("Courts should allow a more general nexus between the prior art and the invention in question to render the latter obvious. . . . After courts make it tougher to satisfy the nonobviousness burden, it will be more difficult to obtain Internet business method patents.").

137. *See supra* notes 119-122 and accompanying text.

138. *See generally* Philip Agre, *Life After Cyberspace*, at http://dlis.gseis.ucla.edu/people/pagre/life.html (visited April 12, 2000) (resisting the temptation to categorize cyberspace as a separate place from the "real world" with a separate canon of law, and instead concluding that cyberspace is better characterized as embedded within the real world of institutions and their social structures).

139. *See* Grusd, *supra* note 106, at ¶ 70 ("For instance, the courts should not allow patents for Internet business methods that merely apply traditional business methods to the Internet. Employing traditional methods of commerce to the Internet may be new and useful, but it is also obvious.")

140. Another similar, but perhaps less radical, idea would be to give less deference to the PTO's determination of a patent's validity in these cases. Instead of giving full deference to the PTO's finding of validity by requiring clear and convincing evidence to prove a patent's invalidity, courts could decide to give deference to PTO findings of validity based *only* on prior art that the PTO actually reviewed. Thus, if pieces of prior art that were never looked at by the PTO are raised at trial, a defendant could more easily prove that an obvious patent is invalid. This effectively would mean reducing the burden to prove invalidity from clear and convincing to a lesser standard in cases where new relevant prior art is brought to light at trial.

141. Victoria Slind-Flor, *The Biz-Method Patent Rush*, National L.J., Mar. 6, 2000, at B7 (addressing the validity of recent viral marketing patents and comparing them to the traditional idea of spreading branding information through word-of-mouth and quoting Professor Rochelle Dreyfuss, who notes that "[t]he notion of using people to tell other people isn't a brand-new idea," explaining that people have worn T-shirts with corporate logos, and restaurants have offered matchbooks bearing their name for many years).

142. *See* Grusd, *supra* note 106, at ¶ 73 (suggesting that "[c]ourts should restrict the scope of business method claims using the enablement provision. This means that courts should carefully examine the claims of each patent in order to determine and mitigate the potential access costs imposed by a broad construction. By reducing the penumbra of each claim, the court can reduce the amount of competition blocking and thus promote efficiency on the Internet.")

143. *See* 35 U.S.C. § 112 ("The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.").

144. It also acts as a backhanded way of ensuring that the "utility" requirement of § 101 is met. If a claimed invention does not actually work, then it cannot enable someone to practice the patent.

145. 56 U.S. (15 How.) 62 (1853).

146. For example, claim 8 would cover televisions, fax machines, and any other telecommunications equipment, but Morse's specification does not describe or enable these applications.

147. *Compare* The Telephone Cases, 126 U.S. 1 (1888) (upholding as valid Alexander Graham Bell's claim 5, which covered "The method of, and apparatus for, transmitting vocal or other sounds telegraphically . . . by causing electrical undulation").

148. *See generally* Richard H. Stern, *Scope-of-Protection Problems with Patents and Copyrights on Methods of Doing Business*, Symposium: IP Rights in Methods of Doing Business, 10 Fordham I. P., Media & Ent. L.J. 105 (1999).

149. *Id*.

150. *See* discussion *supra* Part II.A.1.

151. *See* Gleick, *supra* note 14, at 49.

152. *See, e.g.*, *supra* notes 9-12 and accompanying text.

153. *See, e.g., Interactive Gift Express, Inc. v. Compuserve Inc.*, 47 U.S.P.Q.2d. 1797 (S.D.N.Y. 1998) (patentee unsuccessfully urging claim construction that would broadly extend patent rights over all commercial transactions on the Internet)

154. For a discussion of how the obviousness inquiry functions with respect to new/uncertain technologies, *see supra* note 124 and accompanying text.

155. *See In Re Wright*, 999 F.2d 1557 (Fed. Cir. 1993). The case involved a method of making a non-pathogenic vaccine from a pathogenic virus. The Federal Circuit held that because this is an unpredictable area, it is hard to get assurance from the one example that it has covered the broad claims. Thus, the Court invalidated the patent on enablement grounds. *See also Amgen v. Chugai Pharmaceutical Co., Ltd.*, 927 F.2d 1200 (Fed. Cir.), *cert. denied*, 116 S. Ct. 169 (1991) (patent for method of purifying human EPO bioassay using reverse phase high performance liquid chromatography held invalid for lack of enablement due to the use of the imprecise terminology "characterized by the molecular weight of *about* 34,000 daltons . . . and a specific activity of about 160,000 IU per absorbance unit at 280 nanometers"; court held that the use of "about" in the specific limitation was indefinite and failed to distinguish it from close prior art).

156. For a discussion of the problems raised by this situation, *see* Heller & Eisenberg, *supra* note 94 (discussing the "tragedy of the anticommons" that is raised by situations in which there are multiple small diffuse patent rights that must be maneuvered around to do business).

157. For a list of some of the more widely criticized broad software business method patents, *see supra* notes 8-12 and 82-89 (detailing controversial patents)

158. *See* Amazon.com's U.S. Patent No. 5,960,411, filed September 12, 1997, issued September 28, 1999; *See generally* One-Click Ordering, at http://www.amazon.com/exec/odidos/subst/help/one-click-learn-more.html (visited April 15, 2000).

159. *See* Priceline.com's U.S. Patent No. 5,797,127, filed, September 4, 1996, issued, August 11, 1998.

160. *See, e.g.*, Sightsound Patent No. 5,966,440, filed, June 12, 1997, issued, November 9, 1999.

161. *See, e.g.*, Priceline.com's U.S. Patent No. 5,797,127, filed, September 4, 1996, issued, August 11, 1999.

162. *See, e.g.*, Amazon.com's U.S. Patent No. 5,960,411, filed September 12, 1997, issued September 28, 1999.

163. *See, e.g.*, *Amazon v. BarnesandNoble.com*, 73 F. Supp. 2d. 1228 (W.D. Wash. 1999) (temporarily enjoining BarnesandNoble.com from using Amazon's "1-click" business method on their Web site); *Priceline.com v. Microsoft* (pending suit involving Microsoft's alleged infringement of Priceline's reverse dutch auction patent); *Sightsound v. N2K* (pending suit involving N2K's alleged infringement of SightSound's patent).

164. There is some evidence that change in the PTO has already begun in response to the wave of criticism surrounding many issued broad Internet business method patents that are neither unique or non-obvious. *See* Tim Dobbyn, *U.S. Patent Office to Overhaul Internet Area*, available at http://www.yahoo.com/tech/articles/uspto_overhaul.html (Mar. 29, 2000) (reporting that the U.S. PTO has announced plans to overhaul its scrutiny of Internet business method patents. Changes in the new guidelines, which are to be released shortly, will include standard second reviews of applications and efforts to improve searches of prior art and industry practices).

165. *See In re Zurko*, 142 F.3d 1447 (Fed. Cir. 1998) (en banc) (courts review PTO's findings of validity under a "clearly erroneous standard").

166. *See supra* Part III.A (discussing fears of many commentators and industry leaders regarding these business method patents).

167. This article does not mean to suggest that the Federal Circuit should usurp power that is rightfully held by the PTO. Rather, it suggests that in order to correct for temporary lapses in the PTO, action is required with respect to patents that have issued during that time. Moreover, such scrutiny by the Federal Circuit will encourage the PTO to move quickly to align itself with the proper policies of patent law when analyzing Internet business method patent applications.

168. There are signs that changes are on the way. Due to the vast attention given by the press to many of these contentious patents, the PTO is certainly aware that changes must be made. *See* Dobbyn, *supra* note 164.

169. Heller & Eisenburg, *supra* note 94.

Michael J. Kasdan is a third-year student at the New York University School of Law. **He would like to thank Professor Rochelle Dreyfuss for her guidance and assistance in completing this article, a version of which won First Prize in the 2000 Intellectual Property Law Section Law Student Writing Contest.**

Trade Winds

Trade Winds offers Section members a way to keep up on the comings and goings of their colleagues and upcoming events of interest. Has there been a change in your practice? Any recent or forthcoming articles or lecture presentations? Won any awards recently? Please e-mail submissions to Jonathan Bloom at jonathan.bloom@weil.com.

Welcome New Members:

Henry A. Adcock
Dino Agudo
Angelica Aquino-Gonzalez
Robert F. Bahrampour
Darci J. Bailey
Jennifer Bassuk
Amy Shalimar Bennett
Valerie L. Boccadoro
Jodi B. Brenner
Stephen J. Brown
Frank A. Bruno
Michael Byrne
Maureen D. Calle
David Cancel
Albert Wai Kit Chan
Galal Chater
Ching Wah Chin
Sanije J. Citaku
Noreen L. Connolly
Heidi C. Constantine
Melissa M. Cross
Jeannie V. Daal
Cheryl L. Davis
Serge Debrye
Scott K. Dinwiddie
David B. Dort
Keith R. Eng
Fedra F. Fateh
Neal Feivelson
David Fultz
Kevin Fumai
George M. Gensler
Ann Laura Gisolfi
Reine H. Glanz
Emmanuel E. Gonsalves
Daryl Goodman
Stephanie A. Gore
Karen Greenberg
Takeyoshi Harada
Matthew P. Harper
Yvonne P. Hill-Falconer
Yutonya V. Horton
James Irving
Heather Lynn Jensen
Gail Johnston
Alexandra Kargin
Sita Krafchow
Thomas P. Krzeminski
Richard A. Kurnit
Nancy F. Lanis
Joanne Akiko Liu
Yufeng Liu
Beverly W. Lubit
Frank Maldari
Eugenia Kathryn Martin
Meghan McCurdy
Michael McGraw
Jennifer Meredith
Dana R. Metes
Frederick J. Micale
Gabriel S. Miller
Marc P. Misthal
Cynthia Mitchell
Glenn M. Mitchell
Francis C. Mizzo
Lori-Anne Mooney
Edward T. Moy
Aleksandr M. Muzyka
Jeffrey D. Neuburger
Brian Nolan
Donna Rowley O'Leary
Kenneth D. O'Reilly
Dara L. Onofrio
Daren M. Orzechowski
Steven V. Podolsky
Eric J. Przybisiki
Claudia L. Psome
Thomas A. Rayski
Brendan T. Redmond
David H. Relkin
Paul A. Robbins
Katherine D. Roome
CindyAnn Ross
Charles D. Ruttan
Gerard N. Saggese
Hideyasu Sasaki
Jay P. Sbrollini
Mark C. Scarsi
Wendy Jo Schechter
Jean E. Schreier
Elizabeth M. Schubert
Michael Schunck
Robert Hisashi Shiroishi
Andre Ramon Soleil
Frank J. Spanitz
Shernette Ava Lorraine Stafford
Erich John Stegich
Jenny L. Stewart
Katherine Aurore Surprenant
Jill Taylor
Mark D. Torche
Peter Tsu-Man Tu
Marijke Karin Van Ekris
Christopher Vitale
James R. Vogel
Blaze D. Waleski
James D. Weinberger
Helene T. Weiner
Kristin Brady Whiting
Norman Wise
Joan Xie
Ira L. Zebrak

Save the Date!

New York State Bar Association

Intellectual Property Section

Annual Meeting

Tuesday, January 23, 2001

New York Marriott Marquis

See Program Agenda on Page 50

MEMBERSHIP APPLICATION
New York State Bar Association:

INTELLECTUAL PROPERTY LAW SECTION

Membership in the New York State Bar Association's Intellectual Property Law Section is a valuable way to:

- enhance professional skills;
- keep up-to-date with important developments in the legal profession;
- join colleagues in exciting Section events.

OPPORTUNITIES FOR EDUCATION

The Intellectual Property Law Section offers both the experienced and novice practitioner excellent opportunities to enhance their practical and legal knowledge and expertise. Through Section activities, including conferences on intellectual property (an annual fall event), members may examine vital legal developments in intellectual property law. The Section's Web site provides current information regarding Section events and offers "members only" access to current issues of *Bright Ideas* and current Committee bulletins providing updates on intellectual property law. The Section plans to sponsor continuing legal education (CLE) credit-bearing programs for Section members at reduced rates. Recent programs offered by the Section related to computer software and biotechnology protection, conducting intellectual property audits, and practical considerations in trade secret law. The Section sponsors an annual Intellectual Property Law writing contest for New York State Law Students.

OPPORTUNITIES FOR PROFESSIONAL DEVELOPMENT

Intellectual Property Law Section committees address unique issues facing attorneys, the profession and the public. The Section offers opportunities to serve on committees such as Patent Law; Trademark Law; Copyright Law; Internet Law; Trade Secrets; Technology, Transfer and Licensing; Young Lawyers, and the Special Committee on the Impact of the Uniform Computer Information Transaction Act on Intellectual Property Law.

Committees allow you to network with other attorneys from across the state and give you the opportunity to research issues and influence the laws that can affect your practice. Committees are also an outstanding way to achieve professional development and recognition. Law students are automatically members of the Young Lawyers Committee. Section members may join more than one committee.

A VOICE IN THE ASSOCIATION

The Intellectual Property Law Section takes positions on major professional issues that affect practitioners and advocates those positions within the New York State Bar Association, the legislature, and the public.

See page 48 to become a member of the Intellectual Property Law Section

COMMITTEE ASSIGNMENT REQUEST

Please designate from the list below, those committees in which you wish to participate. For a list of committee chairs and their e-mail addresses, please refer to page 49 of this issue.

___ Copyright Law (IPS1100)
___ Internet Law (IPS1800)
___ Patent Law (IPS1300)
___ Technology, Transfer and Licensing (IPS1400)
___ Trade Secrets (IPS1500)
___ Trademark Law (IPS1600)
___ Young Lawyers (IPS1700)

Please e-mail your committee selection(s) to Naomi Pitts at: npitts@nysba.org

* * *

To be eligible for membership in the Intellectual Property Law Section, you first **must** be a member of the NYSBA.

❒ As a member of the NYSBA, I enclose my payment of $30 for Intellectual Property Law Section dues. (Law student rate: $15)

❒ I wish to become a member of the NYSBA and the Intellectual Property Law Section. I enclose both an Association and Section application with my payment.

❒ Please send me a NYSBA application. No payment is enclosed.

Name _____

Office _____

Office Address _____

Home Address _____

E-mail Address _____

Office Phone No. _____

Office Fax No. _____

Home Phone No. _____

Please return payment and application to:

Membership Department
New York State Bar Association
One Elk Street
Albany, New York 12207
Telephone: 518/487-5577
FAX: 518/487-5579
http://www.nysba.org

Section Committees and Chairs

The Intellectual Property Law Section encourages members to participate in its programs and to contact the Section officers or Committee Chairs for information.

Committee on Copyright Law
Jeffrey Barton Cahn (Co-Chair)
Sills Cummis et al.
The Legal Center
Newark, NJ 07102
Tel: (973) 643-5858
Fax: (973) 643-6500
e-mail: jcahn@sillscummis.com

Robert W. Clarida (Co-Chair)
Cowan, Liebowitz & Latman, P.C.
1133 Avenue of the Americas
New York, NY 10036
Tel: (212) 503-6266
Fax: (212) 575-0671
e-mail: rwc@cll.com

Committee on Internet Law
Rory J. Radding (Co-Chair)
Pennie & Edmonds, LLP
1155 Avenue of the Americas,
22nd Floor
New York, NY 10036
Tel: (212) 790-6511
Fax: (212) 869-8864
e-mail: rjradding@pennie.com

Richard L. Ravin (Co-Chair)
Hartman & Winnicki
115 W. Century Road
Paramus, NJ 07654
Tel: (201) 967-8040
Fax: (201) 967-0590
e-mail: rick@ravin.com

Committee on Patent Law
Philip A. Gilman (Co-Chair)
Kramer, Levin et al.
919 Third Avenue
New York, NY 10022
Tel.: (212) 715-9216
Fax: (212) 715-8216
e-mail: pgilman@kramer-levin.com

Philip A. Furgang (Co-Chair)
Furgang & Adwar, LLP
Two Crossfield Ave., Suite 210
West Nyack, NY 10994
Tel: (914) 353-1818
Fax: (914) 353-1996
e-mail: phil@furgang.com

Committee on Technology, Transfer and Licensing
Walter J. Bayer, II (Co-Chair)
One Independence Way
Princeton, NJ 08540
Tel.: (609) 734-9413
Fax: (609) 734-9899
e-mail:
walter.bayer@corporate.ge.com

Neil Baumgarten (Co-Chair)
1885 Cynthia Lane
Merrick, NY 11566
Tel: (516) 868-6617
Fax: (516) 868-7666
e-mail: nsbaumg@aol.com

Committee on Trade Secrets
Michael B. Carlinsky (Chair)
Orrick Herrington & Sutcliffe, LLP
101 Roundabend Road
Tarrytown, NY 10591
Tel: (212) 506-5172
Fax: (212) 506-5151
e-mail: mcarlinsky@orrick.com

Committee on Trademark Law
Peter S. Sloane (Chair)
Ostrolenk Faber et al.
1180 Avnue of the Americas, 7th Fl.
New York, NY 10036
Tel.: (212) 382-0700
Fax: (212) 382-0888
e-mail: psloane@ostrolenk.com

Committee on Young Lawyers
Marie-Eleana First (Co-Chair)
Law Office of Theodore N. Cox
179 Bennett Avenue, Apt. 1D
New York, NY 10040
Tel.: (212) 925-1208
e-mail: mfirst622@aol.com

Randie B. Rosen (Co-Chair)
Orrick Herrington & Sutcliffe, LLP
666 Fifth Avenue
New York, NY 10103
Tel.: (212) 506-3602
Fax: (212) 506-5151
e-mail: rrosen@orrick.com

Please Join Us for

NEW DEVELOPMENTS IN INTELLECTUAL PROPERTY LAW: A LOOK AT LAW, POLICY AND PRACTICE

Tuesday, January 23, 2001

New York Marriott Marquis • New York City

8:15-8:40 a.m.	Registration (outside meeting room)
8:45-9:00 a.m.	Welcoming Remarks and Section Nominations **Victoria A. Cundiff**, **Esq.**, Section Chair, Paul, Hastings, Janofsky & Walker, NYC Introduction of Program Co-Chairs **Charles E. Miller, Esq.**, Pennie & Edmonds LLP, NYC and **Ray A. Mantle, Esq.**, Brock Silverstein LLC, NYC.
9:00-9:50 a.m.	*State of the Copyright Law—View From the Register's Office* **Marybeth Peters**, Register, U.S. Copyright Office
9:50-10:40 a.m.	*Economic Espionage Act—View From the Dept. of Justice* **Joseph Metcalf, Esq.**, U.S. Dept. of Justice
10:40-11:30 a.m.	*State of the Patent Law—View From the Commissioner's Office* **John Love, Esq.**, Assistant Commissioner, U.S. Patent Office
11:30-11:55 a.m.	*State of the Professional Rules*
12:00-1:30 p.m.	Lunch
1:30-2:00 p.m.	*State of the Future of Intellectual Property Law* **Miriam M. Netter, Esq.**, Mapinfo, Inc., Troy, NY
2:00-3:00 p.m.	*State of the Trademark Law and the Madrid Protocol* **Michael Heltzer, Esq.**, Government Liason, International Trademark Association and **Clark Lackert, Esq.**, Nims, Howes, Collison, Hansen & Lackert, NYC
3:00-3:15 p.m.	Break
3:15-4:05 p.m.	*Patent Law Issues—The Private View* **Steven Weisburd, Esq.**, Ostrolenk, Faber, Gerb, Soffen LLP, NYC
4:05-4:30 p.m.	*Privacy Issues—The Private View*
4:30-4:55 p.m.	*State of Intellectual Property Law in General* Roundtable Discussion by the Speakers and Co-Chairs and Q&A Session
4:55-5:00 p.m.	Recognition of Winners of Intellectual Property Section Writing Competition Prizes **Victoria A. Cundiff**, Esq., Section Chair, and **Walter Bayer, Esq.**, Writing Contest Chair
5:00-6:00 p.m.	Reception Sponsored by THOMSON & THOMSON

For Registration Questions Call (518) 487-5621

2000 Winners

of the Intellectual Property Law Section's

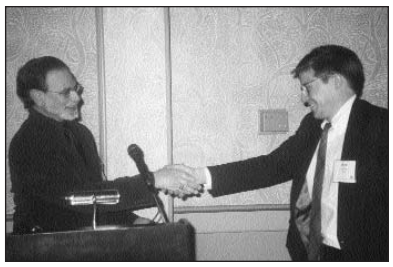
ANNUAL LAW STUDENT WRITING CONTEST

Sponsored by THOMSON & THOMSON

1st Place

Michael J. Kasdan

2nd Place



David R. Johnstone

Honorable Mention

Darryll Towsley

3rd Place: Donna Furey (not pictured)

* * *

Committee Reports

Technology Transfer and Licensing Committee, Trade Secrets Committee, Patent Law Committee

On August 23, 2000, Victoria A. Cundiff of Paul, Hastings, Janofsky & Walker, LLP hosted a joint meeting of the three committees, the Technology Transfer and Licensing Committee, the Trade Secrets Committee, and Patent Law Committee. Philip A. Gilman discussed the key provisions of trade secrets licensing in the Internet age, with a focus on the advantages trade secrets may have over patents in this context.

Young Lawyers Committee

On September, 20, 2000 the Young Lawyers Committee in conjunction with Jacobs, deBrauwere & Dehn LLP and Benjamin N. Cardozo School of Law Center for Professional Development held an Intellectual Property Law Cocktail Reception at Jacobs deBrauwere & Dehn LLP, which was a great success.

* * *

Subscription Information

Bright Ideas is available by subscription to non-attorneys and law libraries. The subscription rate for 2001 is $60.00. Copies of back issues and articles are also available. For further information contact the Newsletter Dept. at the Bar Center in Albany: (518) 463-3200.

Advertising Information

This publication also accepts advertising. The rates for 2001 are: Full Page—$800, Half Page—$500. For further information contact the Newsletter Dept. at the Bar Center in Albany: (518) 463-3200.

Questions and Answers

Members of the state bar who have general questions on any area of intellectual property law can write to us and their questions will be considered by our panel of experts. Questions should be sent to: *Bright Ideas* Q&A, c/o Jonathan Bloom, Esq., Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, New York 10153.

Submission of Articles

Anyone wishing to submit an article, announcement, practice tip, etc., for publication in an upcoming issue of *Bright Ideas* is encouraged to do so. Articles should be works of original authorship on any topic relating to intellectual property. Initially, submissions may be of any length.

Submissions should preferably be sent on a 3.5" disk (double or high-density) which clearly indicates the word processing program and version used, along with a hard copy or by e-mail to Jonathan Bloom, Executive Editor, at the address indicated on this page. Submissions for the Spring/Summer 2001 issue must be received by February 22, 2001.

At-Large Members of the Executive Committee

Kenneth A. Alder
Robert Raney Kiesel
Raymond A. Mantle
Charles E. Miller
Miriam M. Netter

BRIGHT IDEAS

Editor-in-Chief
Rory J. Radding
Pennie & Edmonds LLP
1155 Avenue of the Americas, 22nd Floor
New York, NY 10036
e-mail: rjradding@pennie.com

Executive Editor
Jonathan Bloom
Weil, Gotshal & Manges LLP
767 Fifth Avenue
New York, NY 10153
e-mail: jonathan.bloom@weil.com

Assistant Editor
Walter J. Bayer, II
GE Licensing
One Independence Way
Princeton, NJ 08540
e-mail: walter.bayer@corporate.ge.com

Section Officers

Chair
Victoria A. Cundiff
Paul Hastings et al.
75 East 55th Street
New York, NY 10022
e-mail:vacundiff@phjw.com

Vice Chair
Marc Ari Lieberstein
Ostrolenk Faber et al.
1180 Avenue of the Americas, 7th Floor
New York, NY 10036
e-mail:mlieberstein@ostrolenk.com

Treasurer
Richard L. Ravin
Hartman & Winnicki, PC
115 West Century Road
Paramus, NJ 07654
e-mail:rick@ravin.com

Secretary
Michael B. Carlinsky
Orrick Herrington & Sutcliffe, LLP
101 Roundabend Road
Tarrytown, NY 10591
e-mail:mcarlinsky@orrick.com

Bright Ideas is a publication of the Intellectual Property Law Section of the New York State Bar Association. Members of the Section receive a subscription to the publication without charge. Each article in this publication represents the author's viewpoint and not that of the Editors, Section Officers or Section. The accuracy of the sources used and the cases, statutes, rules, legislation and other references cited is the responsibility of the respective authors.

ISSN 1530-3934

Intellectual Property Law Section
New York State Bar Association
One Elk Street
Albany, NY 12207-1002

ADDRESS SERVICE REQUESTED

NON PROFIT ORG.
U.S. POSTAGE
PAID
ALBANY, N.Y.
PERMIT NO. 155