LEGAL ISSUES IN A DOTCOM COPYCAT CASE

Jerry Wegman
University of Idaho
Academy for Studies in Business Law Journal Vol. 4, No. 2, 2001. Distinguished Research Award winner, Allied Academies 2001

ABSTRACT

The Internet and e-commerce have revolutionized communications and business. Innovative dotcom companies have pioneered new business models and methods. However once a particular business model has proven to be successful, it is often plagued with numerous copycats. Some are legitimate, taking only the basic concept, for example selling wine on line. Others however go further, taking not only the general concept but also stealing the leader's customer list, violating other trade secrets and infringing on its trademarks, service marks, patents and copyrights. When such conduct occurs, the leader must assert its legal rights or see its business stolen. This article will describe the legal rights and remedies available to a dotcom company in that situation. A scenario will be used for illustration. This scenario is based on a real case currently in litigation. The records of that case have been sealed by court order, so names and particulars have been changed. First the scenario will be presented. Then legal issues will be explored including both civil and criminal liability. Next the facts of the scenario will be applied to the legal issues and discussed. Finally conclusions will be drawn, including practical suggestion for dotcom or tech companies that have valuable intellectual property to protect.

INTRODUCTION

In the past six years e-commerce has blossomed. Thousands of innovative and talented entrepreneurs have devoted their fortunes and large portions of their lives to create new web based businesses. These businesses exist largely in cyberspace. Unlike an earlier industrial age, dotcoms of the information age can not point to massive industrial structures or other tangible assets. Their assets consist largely of new ideas, processes, trade symbols, software and goodwill built up by satisfying customer demands. These assets are legally considered intellectual property (IP). IP must be protected with the same vigilance as tangible property.

Ironically digital copying and the Internet, which made possible these new innovative companies, also make it extremely easy to misappropriate IP. An unethical company can use a competitor's trademarked terms to lure customers to its site. It can violate copyrights by placing visible or hidden text on its site. It can confuse customers by copying the look and feel of a popular site. And it can steal the customer lists of its competitors.

The following scenario illustrates how a real dotcom company was confronted with this abuse. As will be seen, this company acted prudently to secure its legal rights in some areas, but it failed to do so in others.

SCENARIO

"Dutch" McDonald, CEO and founder of BoatBuyer.com Inc. leaned back comfortably in his plush leather executive chair. He had just reviewed the latest monthly report of operations. Paid services to boat brokers, site registrations by potential boat buyers, fees for online boat valuations and reviews, and site visits were all substantially up. Most important, profits were up 20% for the quarter. Unlike many of the recently burned out dotcoms, Dutch had insisted from the start on maintaining profitability. The business was frugally run out of three converted residences in an unfashionable part of town. No one, not even Dutch, had a plush office. His leather executive chair was Dutch's only indulgence. But the company's balance sheet and performance chart were stellar: no debt, and steady profit growth averaging 50% a year for the four years since startup.

Dutch's moment of reverie was interrupted by Gary Jobson, his chief tactician and strategist. "Dutch, I think we have a problem with this new competitor, Pirate.com. Their site comes up right next to ours on seven search engines. I checked it out, and it looks a heck of a lot like ours. Same services to boat brokers, articles on sailing, classified listings, the works. And get this: when I had legal check out their officers, who do you think was listed as CEO? Ben Arnold, who quit six months ago. I think we got a copycat".

Dutch was stunned. He immediately checkout out the Pirate.com site and discovered that the situation was even worse than Gary had described it. The look and feel of that site, even the colors used, were identical to his own. The hundreds of thousands of dollars that BoatBuyer.com had spent on site development had been stolen by a rival. Dutch felt the sting of being the victim of a theft. He worried that his customers would be confused and go to the rival's site by mistake. And what if more copycats appeared? His niche business could be eroded, even killed. Dutch immediately scheduled an emergency meeting of all officers and arranged to have Clarence Darrow, BoatBuyer.com's attorney, attend.

The meeting took place next day. "Folks", Dutch began, "We have a serious problem. Yesterday Gary came to me with a copycat site, Pirate.com. I checked it out, and there is no doubt about it: Same site design, same look and feel, same services even the same colors. I called fifteen of our broker-customers this morning, and every one of them had been solicited by the copycat. I think Ben stole our business when he quit six months ago. He may have even stolen our customer list". Gene Hackman, BoatBuyer.com's chief technology officer, spoke next. "After Dutch told me about the copycat I went to their site and viewed its underlying source code. And get this: they were using our trademarked terms "BoatTender" and "BoatsForYou" as part of their metatag! So search engines would give them a high placement if anyone looking for us searched those terms. And here is a new one on me: I found hidden text on their site". Clarence asked: "What is hidden text?" "Its text printed white on a white background. So no one can see it. And the text was a word-for-word copy of our home page!" Clarence was perplexed. "If people can't see it what good does it do?" Gene explained: "the search engine sees it. That's another reason why the copycat places close to us on searches."

The officers all turned to Clarence. Dutch spoke: "Clarence, we're being ripped off. What can we do?" Clarence looked up from the yellow pad on which he had been taking notes. He spoke slowly. "Dutch, you have built up a great little business here. But looking around, I don't see factories, piles of inventory, warehouses. Your business consists primarily of intellectual property. Intellectual property, or IP, is invisible but can be incredibly valuable. And just like physical property, you have to protect it. There are four traditional legal

protections that are available, and also some new ones that Congress has created in the last few years. Lets start with a traditional protection, trade secrets. Your customer list probably qualifies as a trade secret. How was it protected?

Gene replied. "I am in charge of computer security. Access to the customer list is by password and only from two desktop machines: mine, and Dutch's. We are the only ones with the password." Dutch: "Say Gene, when you went to that computer security conference last April, didn't Ben cover for you and use your office for a few days? And that would be about a month before he quit". "Yes, that's true, but he would still need the password, and I never gave it to him. I'll back-track my machine and see if that data was accessed while I was away".

Clarence continued. "Trademark is another traditional protection. Gene, you said that certain Trademarked terms were contained in the copycat's metatag. As I understand it, a metatag is part of a site's source code that contains words a search engine looks for, but are not visible on the site". Gene nodded. Clarence said: "Recent cases have established that using a competitor's registered trademark in a metatag constitutes infringement. We have a solid case there."

"The third traditional protection of IP is copyright. Some people even think that copyright protection has gone too far, lasting as it does today the lifetime of the author plus seventy years." Dutch asked "Is the word-for-word copy of our home page in hidden text a copyright violation?" "Well Dutch, that is a hard question to answer. Fact is, much of the law regarding the Internet is new or in formation. What we lawyers call 'unsettled'. If the copied material were visible, there would be no problem; we would have publication. But seeing as how – that is, not seeing the hidden text, a court might declare that no publication has occurred. There is no clear precedent on this yet, but my guess is that courts will follow the line of reasoning in the metatag cases and find copyright infringement.

Dutch spoke up. "You said there were four traditional protections. What is the last one?" "The fourth is patent. Patents are usually associated with machines, chemicals, or other tangible things. But recent cases have held that Internet based business processes, like Amazon's one-click checkout, can qualify for patent protection. Has BoatBuyer.com applied for or received any patents?" Dutch replied: "You know, we have developed some innovative techniques but I never thought of patenting them." Clarence said "Dutch, there are some Internet companies that have made more money from their patents than from their operations. If you like, I can get together later with Gene to see what we can do."

"As I said, Congress has passed some new laws to protect IP" Clarence continued. "You all know, what with Napster, MP3 and other sites, plus the perfect clones possible with digital copying, IP rights are vulnerable now as never before. The entertainment and software industries have leaned on Congress to shore up their IP rights. They make a good case, especially considering that IP is one of America's leading exports." "Do any of these new laws carry criminal penalties?" Dutch asked. "Arnold doesn't have much money, so a big judgment would be uncollectable against him". Dutch paused. His eyes narrowed and his jaw muscles tensed. "I made that little pimp what he is today. Gave him his first net job and showed him the ropes. Then he betrayed me. Stole from me, stabbed me in the back." The room was silent. Clarence replied. "There are some recent federal statutes that make theft of IP a federal crime. I'll check it out. And I still have some friends in the U.S. Attorney's Office".

"One final question" said Clarence. "Did BoatBuyer.com require Ben Arnold to sign a non-compete or non-disclosure agreement, and does BoatBuyer.com have a written policy about removing proprietary IP from the premises?" Dutch looked up. As an honest man, he expected

others to be honest. "That's three questions, Clarence. And the answer to all three is 'no'. I guess we have been a little naïve". "Welcome to the world, Dutch" said Clarence.

After the meeting Dutch directed Clarence to file a civil action against Pirate.com Inc. alleging misappropriation of trade secrets, and trademark and copyright infringement. A separate civil action was also filed against Ben Arnold alleging theft of trade secrets and violation of the fiduciary duties of an agent. Dutch requested that Clarence meet with federal prosecutors in an effort to have criminal charges brought against Pirate.com and Ben Arnold.

After filing civil actions, Clarence went to his regional U.S. Attorney's office seeking criminal prosecution under federal law. He met with John Dean, the Assistant U.S. Attorney assigned to review the matter. "John, I've laid out a clear case of violation under the Economic Espionage Act and the No Economic Theft Act. Will *you* act?" John smiled at the pun. "Clarence, we have 35 lawyers in this office, and about 50 U.S. Marshals for investigation. Against that we have a caseload of about 2500 major federal felonies a year, from bank robbery and kidnapping to securities fraud. You know we can't try every case. And if it turns out that BoatBuyer.com did not adequately protect its customer list, it's not even a trade secret, so there is no theft to prosecute". Clarence persisted. "John, there were only two machines that had that list, and only two people with the password. Isn't that at least reasonable protection? Sounds like an airtight cast of violation of the Economic Espionage Act to me". John asked: "Then how did Arnold get that list?" "We have evidence that he hacked it. Which would also violate the federal computer fraud statute." John was silent for a minute. "Let me see that brief again, with your list of evidence. We may be able to do something here … I'll check with the bureau chief on policy and resources. No promises, but we might move on this one."

Clarence was relieved. As a former prosecutor himself, he knew that it is a matter of discretion for the prosecuting attorney whether to bring a criminal case in the name of the government. Clarence understood that the likelihood of conviction and seriousness of the crime must be balanced against the costs of prosecution, including alternative opportunity costs.

The civil action proceeded with discovery. Ben Arnold was first to be deposed. He was confronted with evidence that Gene's computer had been compromised while Ben had been temporarily occupying Gene's office. Ben finally admitted to hacking the customer list. "How did you obtain the password?" asked Clarence. Ben explained that it was easy. "I tried several obvious combinations and when I tried Dutch's name and birthday, I was in". The depositions, plus documents produced pursuant to court order established that Pirate.com's programmers had indeed used BoatBuyer.com's site as a model, and had copied much of its source code verbatim. Nevertheless the copycat maintained that there was enough original material to avoid copyright violation. Ben claimed that when he took the BoatBuyer.com customer list he was entitled to do so, as he was then an officer of the firm. BoatBuyer.com demanded damages of $5 million and a consent decree to permanently cease and desist from violating its IP. The copycat refused and the matter was set for trial, which is scheduled for early next year.

LEGAL ISSUES

1. Copyright.

Copyright is perhaps the most important legal protection of software and Internet information. Copyright protects "original works of authorship" including "literary works … sound recordings … motion pictures"[1]. The 1980 amendment to the Copyright Act added

computer software to copyrightable works.[2] Copyright law is governed by the U.S. Copyright Act[3], also known as the Lanham Act (which also affects trademark). The federal act preempts state law. Copyright confers on its owner exclusive right of use. In effect, the owner has a temporary monopoly on the copyrighted work. Copyright and patent share the distinction of being enshrined in the U.S. Constitution. Article I, Sec. 8 grants Congress the power "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries".

The Internet and computers have posed new challenges to copyright. The Internet has been described as "a gigantic international copying machine".[4] The Internet and computers have made it easy to make digital copies that are identical to the original. The entertainment and software industries are particularly threatened by this. These industries have lobbied Congress to strengthen their intellectual property rights. As a result, the Copyright Act was amended in 1980, 1990, 1998 and 1999. The Act now provides extensive and lengthy legal protection, but enforcement is problematical.

The 1998 amendment, also known as the Sonny Bono Copyright Extension Act, extended the duration of copyright an additional 20 years. Duration of copyright depends upon whether it is held by an individual or a corporation. An individual's copyright protection now lasts the lifetime of the author plus 70 years. A corporation's copyright protection now lasts 120 years from the year of first creation, or 95 years from the year of first publication, whichever is shorter. Some feel this is excessive[5].

Copyright protection is extended to "original works of authorship fixed in any tangible medium of expression … from which they can be perceived …"[6]. There was originally some question as to whether Internet programs were sufficiently "tangible" but now it is settled law that they are copyrightable. It is permissible to register an entire web site with the U.S. Copyright Office and this is a good idea, as discussed below.

Registration of copyrighted work is not absolutely required but it is highly recommended. If the work is not registered copyright protection begins as soon as the work is fixed in a tangible medium. But the burden of proof as to whether and when that occurred is on the author. A copyright notice, while no longer absolutely required[7], is useful to refute a claim of innocent infringement. Registration is highly recommended also because it gives the plaintiff the right to bring an action in federal court based on the Lanham Act and to recover statutory damages under the Act. The Act allows recovery of actual damages suffered plus profit made by the infringer. It also provides the option of awarding statutory damages in lieu of actual damages. Statutory damages were increased by the 1999 amendments to a maximum of $30,000 per work infringed.

The Copyright Act is a strict liability statute: no proof of intent is required. However, if the copyright holder is able to prove an intentional, willful infringement, statutory damages go up to $150,000 per work infringed plus reasonable attorney's fees. In addition to monetary damages the court can also order the destruction of infringing works and issue an injunction preventing future infringement.

In order to prove infringement, the copyright holder must first show that he or she owns the copyright. Registration makes that easy. Infringement can be proved either by direct evidence of copying or by inference. In most cases infringement is proved by inference where the copy is substantially similar to the copyrighted work and the defendant had access to it.[8]

The most important recent case of copyright infringement in the technology area is *Computer Associates International, Inc., v. Altai, Inc.*[9] The facts of that case bear some similarity to the facts of our scenario. In *Computer Associates*, a computer programmer, Arney,

developed a software product for CA. He was later hired by a competitor, Altai. Arney had been permitted to take home copies of the source code for various CA products while he was employed there. Upon leaving that firm, he took with him copies of CA source code for various products, including one called ADAPTER that he had developed. While at his new firm, he was asked to develop a product similar to ADAPTER. No one at Altai knew that Arney had developed a similar product for CA and no one knew that he still had the source code for that product. Arney produced the new product for Altai. It was named OSCAR 3.4, and contained about 30% of the source code of ADAPTER, copied by Arney without the knowledge of Altai personnel. After three years CA learned of the copying and sued Altai for infringement. So far the case is easy. The District Court found a direct infringement during those three years and awarded damages of $364,444. It stated the settled legal rule as follows:

> In any suit for copyright infringement, the plaintiff must establish its ownership of a valid copyright, and that the defendant copied the copyrighted work (cases cited). The plaintiff may prove defendant's copying either by direct evidence or, as is most often the case, by showing that (1) the defendant had access to the plaintiff's copyrighted work and (2) that defendant's work is substantially similar to the plaintiff's copyrightable material (cases cited).[10]

What makes this case interesting is the response of Altai to being informed of the copying. Altai first became aware of it when it was served with the summons and complaint by CA. Altai's president, Williams verified the accuracy of the claim, then immediately removed Arney from the OSCAR project and put six other programmers to work writing original source code to replace the copied code. These new programmers had no previous experience with OSCAR and did not see the source code for OSCAR 3.4 or for ADAPTER, which Williams locked away. After six months the new programmers had developed original source code to replace the copied material. Altai then released OSCAR 3.5 and provided it as a free upgrade to users of OSCAR 3.4.

In spite of Altai's admirable efforts to cleanse itself of the infringed material, CA claimed that OSCAR 3.5 also violated its copyright. CA claimed that although there was no literal copying of CA material on OSCAR 3.5, there was access to ADAPTER and also "substantial similarity" to it because of similar structure, sequence and organization. Some earlier cases had accepted this theory of infringement[11]. However, in *Computer Associates* the court held that even though access and similarities existed, the strong evidence of original work in that case overcame the inference of copying with respect to OSCAR 3.5.

It should be noted that the *Computer Associates* case is unusual. In most cases the infringing firm is unable to overcome the inference of copying that results form access and substantial similarity. This case provides a good example of how an ethical firm should respond when it discovers that one of its employees has violated a copyright. Not only is it an ethical response, it also minimizes the resulting liability.

2. Patent

As noted above, the framers of our Constitution recognized the importance of encouraging and protecting "Writings and Discoveries". The current federal statute governing inventions is the Patent Act of 1952[12]. To qualify for patent protection, the invention must be

novel, useful and non-obvious[13]. Ideas, concepts, and formulas such as $e=mc^2$ are not patentable. Until World War II patents were issued only for tangible things including "process, machine, manufacture, or composition of matter, or any new and useful improvement thereof"[14]. The industrial Age produced tangible inventions like the light bulb.

With the coming of the Information Age invention included intangible products like computer software. American courts were slow to allow patentability of these new forms of invention, considering them mere ideas and formulas and therefore not entitled to patent protection. The landmark 1972 U.S. Supreme Court case of *Gottschalk v. Benson*[15] illustrates this. The inventor had developed an algorithm for converting decimal numbers into binary numbers. Such an algorithm is a necessary part of the software used by almost every computer. An earlier algorithm existed, but it was less efficient than the new one. The Patent Office rejected the application because it considered it a mere mathematical formula. The U.S. Supreme Court agreed. This led to the general conclusion both in the United States and Europe that computer software was not patentable.

In 1981 the U.S. Supreme Court reversed itself. *Diamond v. Diehr*[16] held that some computer software programs were patentable. In that case the court considered the patentability of a process for making synthetic rubber that included a computer program for determining the exact time the rubber needed to stay in its mold. The Supreme Court held that because that computer software program was part of a useful process, it was patentable along with the other parts of that process. This was a breakthrough case and led to the widespread use of patents for computer software.

Recently the courts have expanded patent protection to include Internet business processes and models. The patentability of Internet processes and business models is a hotly debated topic. Some critics complain that many such patents are obvious should not have been granted[17].

This is well illustrated by the famous case of *Amazon.com, Inc. v. Barnesandnoble.com, LLC.*[18] This case tests whether Amazon's "one click" checkout patent was valid. Amazon had developed a software-supported process that enabled a customer to order, purchase, and ship an item just by clicking on one button. This required that the customer had previously registered giving shipping address and credit card information. The one click process made purchase easy and it solved a major problem of e-commerce: the "abandoned shopping cart" problem. Customers would often complete the checkout process part way and then quit.

Barnesandnoble challenged the patent on two grounds: that it was obvious, and that prior art existed for the same invention. At a hearing in 1999 to determine whether a preliminary injunction should be issued, Amazon introduced evidence showing that although in hindsight the one click process might seem obvious, at the time of invention no one else had thought of it. The process is commercially significant because it proved very popular and helped solve the abandoned shopping cart problem. Barnesandnoble's similar "Express Lane" feature, with one click checkout, was also popular. Amazon also introduced evidence suggesting that prior art did not anticipate Amazon's one click process. The District Court was persuaded that Amazon was likely to prevail and that irreparable harm would result unless a temporary injunction was issued. Accordingly, it issued a preliminary injunction against Barnesandnoble. The decision to issue a preliminary injunction in favor of Amazon's patent provided a big boost to those claiming such patents. The U.S. Patent Office became more receptive to them and many were issued. [19]

Most recently however the legal landscape has again shifted. On February 14, 2001, the U.S. Court of Appeals for the Federal Circuit reviewed the issuance of Amazon's preliminary

injunction and set it aside[20]. In setting aside the preliminary injunction the Court of Appeals stated that it disagreed with the District Court's conclusions as to the likelihood of Amazon's ultimate success defending its patent. The Court of Appeals felt there were "substantial questions as to the validity of the … patent" because of prior art and obviousness. It remanded the case for trial on the merits, which will test the validity of Amazon's patent. Trial is now scheduled for September 2001.[21]

The recent spate of Internet patents has drawn criticism from some who claim that they are not warranted, that they increase costs to e-commerce generally and that they generate unnecessary litigation expense.[22] Even Jeff Bezos, president of Amazon, has said "I now believe it's possible that the current rules governing business methods and software patents could end up harming all of us"[23].

3. Trademark, Service Mark

A trade symbol informs consumers of the origin of goods and services. It also protects the goodwill that a firm has developed. Trademarks and service marks are among the four trade symbols that are recognized by the Federal Trademark Act[24], also know as the Lanham Act. Trademarks can also be protected under state law. Trademarks should be registered. The U.S. Office of Patents and Trademarks (OPT) is the preferred registrar because in order to sue in federal court and to obtain the benefits of the Lanham Act the marks must be registered with the OPT. Federal registration lasts ten years but is infinitely renewable. If the infringement is intentional, treble damages plus reasonable attorney's fees may be awarded.

Most cases of trademark infringement involve confusion and diversion of customers to the infringing firm. Recently a new form of trademark abuse has surfaced. This consists of using another's trademarked terms as part of the metatag of a web site, invisible to the site visitor.

A metatag consists of source code imbedded in the hypertext markup language (HTML) of a web site. It is invisible to the site visitor but a search engine "sees" it and uses it to place it appropriately in a search. It may be viewed as follows: using Netscape Communicator 4.7, go to a site e.g. eBay, then click on the "view" button and choose "page source". The HTML will be displayed. At the top of the HTML the "meta name" lists the metatags associated with that site. Ebay's metatag terms include "auction", "bid", and "memorabilia". A customer entering those terms in a search engine would find eBay among the first sites listed.
An unethical dotcom could include a competitor's trade name or trademarked terms in its metatag. This would cause a customer looking for the legitimate business to go to the infringing site. Once there, the customer would realize the error, but might be enticed to do business at that site. This has been described as "invisible trademark infringement"[25].

There have been several cases in which the trademarked terms "playboy" and "playmate" have been used in the metatags of unauthorized porno sites. Perhaps the best known case is *Playboy Enterprises, Inc. v. Terri Welles, Inc.*[26] This is the leading case dealing with "fair use" of another's trademark on the Internet.[27] Ms. Welles had appeared on the cover of Playboy magazine in May 1980, and had been "Playmate of the Month" in December 1980 and also "Playmate of the Year" in 1981. In 1997 Ms. Welles opened a web site that included nude photographs of herself. The metatags for her site included the terms "playboy" and "playmate". Playboy sued alleging, among other things, infringement of its trademarked terms used in the metatags of Welles' site.

Judge Keep noted that metatag infringement differed from conventional infringement in that the confusion is of a type that will not cause the consumer to think he or she is doing business with another firm. Rather, it is "initial interest confusion: a confusion of consumer attention, even though no actual sale is finally completed as a result of the confusion"[28]. Earlier cases, including *Dr. Seuss Enterprises V. Penguin Books USA, Inc.*[29] and *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*[30] had held that use of another's trademark in a metatag could constitute infringement. Judge Keep in *Welles* held that a finding of infringement was not an automatic result from the use of another's trademark in a metatag. For the first time, a federal court held that such use could constitute legitimate "fair use", analogous to the fair use of copyright. If the metatag is a fair description of the site, is not "damaging and wrongful", will not cause the consumer to believe there is a connection with the trademark firm, or cause that firm to lose customers, then use of the other's trademark in a metatag is legitimate fair use.

Because Ms. Welles had indeed been a playboy playmate someone looking for her site but not remembering her domain name might enter "playmate" in a search engine. In the *Welles* case there was no evidence of intent by Ms. Welles to imply a connection to Playboy. In fact, her site contained numerous disclaimers of any such connection. There was no evidence of lost customers or other damage to Playboy. Accordingly, Judge Keep denied Playboy's claim of infringement.

It is well to note that the *Welles* case is the only case so far that had held use of another's trademark in a metatag to be fair use. It is an important case in that it delimits the boundary between legitimate fair use and unlawful infringement of trademark in metatags.

4. Trade Secrets

Sometimes copyright, patent and trademark are either unavailable or not good choices for protecting intellectual property. If the IP is not a "creative work" it is not entitled to a copyright. Mere lists such as customer lists are not considered creative works, unless perhaps they are arranged in a particularly creative way[31]. A trademark or service mark can only protect certain distinctive terms or terms that have acquired a "secondary meaning"[32]. They must have been properly registered and renewed. A patent will only be issued if it is novel, useful and non-obvious. Patents expire after 20 years, and once a patent is issued it becomes public knowledge. It is easily available to anyone who conducts a patent search. Encryption breaking hackers often conduct a patent search to find out how to break anti-copying software[33].

When other protections of intellectual property are either unavailable or unsuitable, trade secret protection may be a good choice. If information legally qualifies as a trade secret, then it is the private property of its owner and protected potentially forever. The formula for Coca-Cola, which was first used in 1886, is perhaps the best example of this. On the other hand, if the secret is discoverable by reverse engineering, trade secret would bee a poor choice.
The Uniform Trade Secrets Act[34] (UTSA) states that in order to qualify as a trade secret, two elements must be present. The first is "independent economic value … from not being generally known". The second is that it must be protected by "efforts that are reasonable … to maintain its secrecy"[35].

Independent economic value is relatively easy to establish. Information which is commonly sold or leased, such as a list of persons interested in a particular product or service, has independent economic value. Reasonable efforts to maintain secrecy may be more difficult

to establish. Such efforts usually involve expense and inconvenience. Safes, security systems, limited access and passwords all add cost and inefficiency. A problem with passwords is that users tend to choose ones that are easy to remember. This also makes them easy to hack.

Once a plaintiff establishes that the information qualifies as a trade secret, a "misappropriation" must be proved. UTSA Section 1 defines misappropriation as obtaining through "improper means". Both the person who acquired the secret and also the person who knowingly received the secret are liable. Damages can be substantial. They can include both the actual loss caused by the misappropriation and also the gain to the defendant. Alternatively, damages can be calculated based on what a reasonable royalty might have been. If the court finds that the misappropriation was "willful and malicious", exemplary damages equaling up to twice the actual damages can be added, and the court can also award reasonable attorney's fees. Thus it is possible to recover three times the actual damages plus attorney's fees where the misappropriation has been willful and malicious.

While misappropriation of trade secrets is unlawful, it is perfectly legal for a former employee to use general knowledge and skill gained at that former employment. Trade secrets law tries to strike a reasonable balance between protecting a firm's intellectual property rights and a former employee's right to earn a livelihood. A case that illustrated this is *Vermont Microsystems Inc. v. Autodesk, Inc.*[36] A software designer who was the self described "chief architect" of a major software product left his employer. He then went to work for a competitor and developed a similar product. The court acknowledged his right to use the skill obtained previously, but held that the two software products were so close that copying could be inferred. This case also illustrates the importance of non-compete and non-disclosure agreements, discussed below.

Another interesting recent trade secret case is *Ed Nowogroski Insurance, Inc. v. Rucker*[37]. This case involved former employees of an insurance agency who misappropriated its customer lists then solicited business from those customers. The employees argued that they had not "taken" anything because they had memorized the lists and had the information in their heads. The court rejected that argument.

5. Non-Competes, IP Policies and Employment Contracts

Non-compete and non-disclosure agreements, written IP policies, and properly drawn employment contracts can be invaluable when dealing with the problem of former employees misappropriating IP.

Employee turnover is inevitable. The dotcom employee who leaves is capable of taking proprietary source code, trade secrets and knowledge of new products and strategies. The departing employee also takes with him or her the personal goodwill that has been built up with customers, suppliers and others. All of these can be turned against the original employer if the former employee goes to work for a competitor or starts a competing business. Courts have held that an employer is entitled to reasonable protection from such abuse.[38] On the other hand, the courts have also held that an employee must be reasonably free to pursue employment and he or she is entitled to use the skill and knowledge gained at one firm when working for another firm.[39]

The issue of employees competing with their former employers is ancient and has generated well-settled law. Applying this settled law to the Internet requires no special modifications except to point out the importance of having non-compete agreements. Courts will enforce such agreements if they are reasonable. The test of reasonableness contains three

elements: First, how long a period of time the employee is being restrained. Second, how extensive is the geographic area in which the employee is being restrained. Third, what kinds of work are being restrained.[40]

With regard to the period of time, one to two years has generally been held to be reasonable. With regard to the geographic area, the courts insist that the area in which competition is being restrained must not be greater than necessary. A local business, e.g. a bakery, could reasonably restrain a former employee from competing within the local area, but not 500 miles away. The bakery will suffer no loss of business from such a distant competitor. The technology sector presents, in many cases, a world-wide market. Where competition is truly global, it would be reasonable to restrain competition globally. With regard to the kind of work the employee has engaged in, the court will limit restraint on competition to those kinds of work in which the employee has gained access to trade secrets or other proprietary information.[41] For example, a computer programmer may have been working on missile guidance systems for a defense firm. That firm could enforce a non-compete agreement that prevents the employee from doing that same type of work. But the employee is free to go work for another firm developing word processing software.

Every Internet company should require its employees to sign appropriate non-compete agreements. It should also develop a written IP policy and make it known. The *Computer Associates* case described above illustrates the need for this. In that case employees were permitted to remove proprietary source code from the business premises. This made it easy for a departing employee to take it with him or her. A clear policy that limits employees' right to copy or remove IP might discourage abuse by employees and is probably necessary to maintain the trade secret status of certain IP. Violation of the policy could provide legal grounds for termination, which otherwise might provoke a counterclaim of wrongful termination by the employee. The IP policy should be reinforced by exit interviews and contact with the new employer. This might also discourage misappropriation of IP, and if it does not it will help to prove willful infringement, which carries greater liability than innocent infringement.

Employment contracts should be written to include non-compete agreements, non-disclosure agreements, promises to abide by the firm's IP policies, and agreements that recognize the firm's ownership of any IP created by the employee.

The employment contract should also cover the topic of proper use of the firm's computer equipment and Internet access. Downloading of pornography or gambling can be made the basis for termination. Many firms spot check employees' use of equipment to make sure it is being used for business purposes. Court decisions support this kind of surveillance, so long as it has a legitimate business purpose. For example, in *Smith v. Pillsbury*[42] the court denied a wrongful termination claim by an employee who had been fired after employer surveillance discovered offensive email on his office computer. The court held that he had no reasonable expectation of privacy. And in *U.S. v. Simons*[43] a federal appeals court upheld a criminal conviction that was based on an employer's search of computers used at work. That court also stated that the employee had no reasonable expectation of privacy. Notifying the employee of the possibility of such surveillance destroys any expectation of privacy the employee may have. Currently three quarters of major U.S. firms spot check email, internet activity and computer hard drives.[44]

As can be seen, the employment contract provides the firm with many opportunities to safeguard its intellectual property. It also provides opportunities to ensure that employees use their computers and Internet connections productively. A prudent dotcom firm will employ

competent counsel to draft appropriate employment contracts and policies that will capture these benefits.

6. Criminal Prosecution

The foregoing discussion of legal issues has been limited to civil law rights and remedies. These are important; they can bankrupt an unethical adversary, and they can compensate a victim for loss and even add exemplary damages plus attorney's fees. But civil law remedies are of little value against a defendant who is without substantial funds. As Bob Dylan once wrote "when you got nothing you got nothing to lose".[45] Against such fly-by-night malefactors the only meaningful deterrent or penalty is criminal prosecution. Congress takes very seriously the crime of misappropriating intellectual property. Dotcoms that have been wronged should do likewise.

The decision to prosecute is a matter of discretion for the prosecuting attorney[46]. The plaintiff in a criminal case is the state; the crime victim is a witness. In exercising proper discretion in the decision to prosecute, the prosecutor will consider the strength of the evidence hence the likelihood of conviction. The prosecutor's burden of proof is "beyond a reasonable doubt" which is a great likelihood, perhaps approaching 98%. This compares with the burden of proof in a civil case which is a mere "preponderance" or a likelihood of approximately 51%. One danger of bringing a criminal case with weak evidence is that acquittal is likely and even if much stronger evidence is later obtained the rule against double jeopardy will prevent a later successful prosecution. The prosecutor must also consider his or her limited resources and give priority to the most deserving cases. Also, as most prosecutors are elected, it is not unknown for political considerations to enter the decision matrix.

In light of the foregoing it is prudent for the corporate victim of intellectual property theft to approach the prosecutor's office with a fairly complete brief including specific criminal statutes violated, manner of violation, identities of the perpetrators and most important of all substantial evidence supporting the claim. If the prosecutor sees that most of the investigative work has already been done a positive decision is more likely.

Congress recently enacted two federal criminal statutes that punish IP theft, and one that makes computer fraud a crime. These will be discussed in turn.

First, the Economic Espionage Act of 1996[47] gave federal prosecutors a powerful weapon against theft of trade secrets. Section 1832 of that Act provides:

> (a) Whoever, with intent to convert a trade secret … knowingly
>
> > (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (or) …
> > (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
> >
> > shall … be fined under this title or imprisoned not more than 10 years, or both.

It will be noted that this section makes criminally liable not only the thief, but also one who knowingly obtains from the thief. Part of a firm's IP policies should include notification of later employers that its former employees may be in possession of proprietary IP and that violation of the firm's trade secrets carries serious criminal penalties that the firm intends to enforce. Quoting the strong language of Section 1832 may have a deterrent effect.

Second, the No Electronic Theft (NET)Act of 1997[48] made copyright infringement a federal crime under certain circumstances. This Act was originally intended to punish or deter music and video copying . Section 506 provides criminal penalties of up to five years imprisonment (ten years for a second offence) for "the reproduction or distribution, of at least 10 copies or phonorecords (sic), of 1 or more copyrighted works, which have a total retail value of more than $2,500". The NET Act would apply if copyrighted software was taken and at least 10 copies were made. If an unethical dotcom copied a substantial portion of a competitor's site and distributed it via the Internet, that would arguably qualify as a violation of the NET Act.

Third, Section 1030 of the federal criminal code[49] makes computer fraud a federal felony. That section provides:

> (a) Whoever … knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value … shall be punished …
> the punishment is a fine or imprisonment for not more than ten years, or both…

The definition of a "protected computer" includes one "which is used in interstate or foreign commerce or communication"[50]. Hacking into a computer to steal trade secrets or other things of value would constitute a violation of this statute if the computer is used in interstate communication or commerce, which almost every business computer is.

DISCUSSION: BOATBUYER.COM

In this section we will discuss the legal issues and practical considerations as they apply to the facts of the BoatBuyer.com scenario.

1. The Customer List

As noted above, to qualify for trade secret protection the secret must have independent economic value and be protected by reasonable security. There can be no doubt that BoatBuyer.com's customer list has economic value. Vendors of boating goods and services can use it to target their marketing efforts at a population of identified boating enthusiasts. The only question that remains is whether the efforts made to maintain the customer list's secrecy constitute reasonable security. By choosing an easily hacked password, it could be argued that the effort fell short. Certainly the legal case would be stronger had a non-obvious password been used. But by also restricting access to only two machines, almost certainly the reasonable security requirement has been satisfied. This also illustrates a problem with password protection: in order to make passwords easy to remember, users often also make them easy to hack.

Damages for misappropriating BoatBuyer.com's customer list could be substantial. Because the misappropriation was willful treble damages plus attorney's fees could be awarded.

In addition, criminal prosecution under the Economic Espionage Act is likely to result in conviction of both Ben Arnold and Pirate.com. Arnold faces a possible jail sentence of up to 10 years, and Pirate.com faces a fine of up to $5 million. The possibility of jail, heavy fines and substantial civil damages is a big incentive to the copycat to settle this case quickly and on terms very favorable to BoatBuyer.com.

2. The Trademarked Metatags

Most cases of trademark infringement involve confusion and diversion of customers to the infringing firm. If the infringement is intentional, the court may award treble damages plus attorney's fees. The BoatBuyer.com scenario is unusual in that the infringer did not use the trademarked terms in an open way so as to confuse customers into thinking they were dealing with BoatBuyer.com. Instead the infringement consisted of using those terms as part of the metatag of its web site, invisible to the site visitor, to lure BoatBuyer.com's customers to Pirate.com's site.

Recent cases, including the *Welles* case discussed above, have established that infringement may result when a website uses a competitor's trademarked terms in its metatag. This emphasizes the importance of registering the firm's marks with the Office of Patents and Trademarks. The Trademark Act provides treble damages plus attorney's fees for willful infringement of registered marks. Use of the trademark symbol or other notice of trademark is useful to refute a claim of innocent infringement.

The circumstances of the scenario provide ample evidence that Pirate.com's infringement was willful and malicious. BoatBuyer.com will likely prevail in its claim of metatag trademark infringement, and it will likely be awarded substantial damages.

3. The Hidden Text

Copyright infringement based on hidden text is a new variation on an old theme. Traditionally, copyright infringement involved publication. With hidden text a defendant would argue that because the hidden text was invisible to site visitors no publication had occurred. A case raising this issue was brought for the first time in July 2001 in Europe. Euregio.net AG filed a case in Brussels against Women.com Networks Inc., alleging copyright violation via hidden text.[51]

Euregio operates a site called EasyScopes.com, on which it publishes a directory of horoscopes. Euregio alleges that Women.com Networks Inc., which operates a site called InternetHoroscopes.com had copied the EasyScope directory almost verbatim onto its site, even including spelling errors. Women.com had printed the directory white on white, invisible to site visitors. Its sole purpose was to boost its standing in searches seeking horoscope sites. After Euregio complained, Women.com removed the invisible text. However Women.com refused Euregio's demand for one million euros ($860,000) in damages. Attorneys are now discussing settlement, so this case might not provide judicial precedent.

Although there is no controlling legal authority on the new issue of hidden text infringement, this author feels it is likely that when courts consider this issue they will follow related precedents finding infringement when metatags are used as the infringing vehicle. Like hidden text, metatags are also invisible to site users. And like metatags, they are also used to lure a firm's customers to a competing site.

In our scenario BoatBuyer.com failed to register its entire site with the U.S. Copyright Office. Had it done so, it would have been entitled to statutory damages in lieu of actual damages. Because the copycat's infringement can be shown to be intentional and willful, statutory damages would be up to $150,000 per infringement.

4. The Visible Copied Text

Copyright infringement has certainly resulted from Pirate.com's copying and use of substantial visible parts of BoatBuyer.com's web site. There is direct evidence of such copying from deposition testimony of programmers who admitted using the BoatBuyer.com site as a model and copying verbatim substantial portions of it. Even without such direct evidence, copying would be implied. Both access and substantial similarity exist. This is not a case of fair use, such as the *Welles* case, but rather a case of willful, malicious infringement with intent to harm BoatBuyer.com. Accordingly, damages will be awarded under state law. As noted above, the failure to register the entire site with the U.S. Copyright Office will result in a smaller judgment than would have been obtained under the Lanham Act.

Copying of the visible text also probably violates the No Economic Theft Act. The copied material was "distributed" to more than 10 site visitors and the copied material can probably be shown to have a retail value of more than $2,500. However, as the intent of that Act is to prevent pirating of entertainment software, a jury might not feel that a conviction is warranted in this case.

5. Potential Patents

Although BoatBuyer.com did not patent its process or business model, it should consider doing so immediately. Patents are recognized as valuable assets. They have been used to obtain venture capital and loans. Patents might discourage certain forms of competition. Alternatively BoatBuyer.com may want to license its patents and generate revenue from them. The current attitude of the Patent Office is permissive with respect to issuing such patents. However, BoatBuyer.com should realize that it may have to defend its patents, and this can be expensive. One author estimates that a patent defense typically costs from $1 million to $1.5 million[52].

6. Criminal Prosecution

If the U.S. Attorney's Office decides to prosecute, a conviction of Ben Arnold and Pirate.com Inc. is likely. The anti trade secret theft provisions of the Economic Espionage Act have almost certainly been violated. Even though an easily hacked password was used, by limiting access to only two computers a reasonable level of protection has probably been demonstrated. The economic value of this customer list is almost self-evident. Arnold's hacking of this list satisfies the requirement of stealing, taking or carrying away.

BoatBuyer.com's chances of interesting a federal prosecutor might have been greater if the defendant had been acting for a foreign corporation. One of the goals of the Economic Espionage Act is to protect U.S. intellectual property from foreign firms. In 1997 F.B.I. Director Louis Freeh stated that $24 billion per year was being stolen from U.S. firms by at least 23 foreign governments or foreign corporations[53].

A current example is the case against three former employees of Lucent Technologies. On May 14, 2001 they were arrested and charged with conspiracy to steal trade secrets from Lucent. It is alleged that the three had planned to set up a Chinese corporation that would produce the same type of equipment manufactured by Lucent.[54]

Conviction under the anti-copyright violation provisions of the No Economic Theft Act is less likely, as discussed above. That Act was intended to thwart piracy of entertainment software. A jury might consider it a stretch to apply it to the facts of this case. In a criminal case any doubt must be resolved in favor of the defendant.

Conviction is more likely under the computer fraud section of the federal criminal code. Arnold certainly acted knowingly and with intent to defraud when he hacked BoatBuyer.com's computer. Evidence will show that he was then planning to set up his competing firm and thus was acting to defraud his current employer. The BoatBuyer.com computer was almost certainly used to communicate with customers in several states, so it qualifies as a 'protected computer' under the statute.

CONCLUSION

The most valuable asset of a dotcom is often its intellectual property. It must act to protect its intellectual property just as it acts to protect its tangible property. Trade secrets must be given reasonable protection, even at some cost. Access to trade secrets should be provided only on a need to know basis. Encryption should be considered. If passwords are used they should be made difficult to hack and they should be changed regularly. Trademarks should be registered with the U.S. Patent and Trademark Office, and renewed on time; this involves routine legal work and is not expensive. The entire web site should be registered with the U.S. Copyright Office; this is also not expensive. If the dotcom has developed a web based business process, a patent attorney should be consulted to determine if it qualifies for patent protection. The firm should have its attorney draw up employment contracts with well-defined non-compete and non-disclosure agreements. It should have a written intellectual property policy that limits taking of proprietary intellectual property from the workplace. The policy should also govern computer and Internet use by employees, and it should advise them of the possibility of surveillance.

When employees leaves, exit interviews should be held to remind them of these legal obligations. It would also be advisable to inform the employee of his or her potential criminal liability under the Economic Espionage Act, the No Electronic Theft Act, and the computer fraud section of the federal criminal code. Subsequent employers should be contacted and informed of the type of work performed by the employee and of the employee's access to proprietary intellectual property.

Doing all of the above will not guarantee that the firm will achieve complete protection for its valuable intellectual property, just as the finest lock will not guarantee complete protection against a break-in. However, it is foolish not to take advantage of one's rights. As always in our society, it is left to the individual first to become educated as to his or her rights, and then to assert them.

ENDNOTES

1 Copyright Act of 1976, 17 U.S.C. Sec. 101 *et seq.* as amended 1980, 1990, 1995, 1998 and 1999.

2 *Id.* Sec. 101.

[3] *Id.* note 1.
[4] Jeffrey Garten, *Intellectual Property: New Answers to New Questions,* BUSINESS WEEK (April 2, 2001).
[5] Robert Kutter, *Sorry, But The New Economy Demands New Regulations,* BUSINESS WEEK (July 30, 2001).
[6] Copyright Act, Sec. 102 (a), 15 USC 1051 (1976).
[7] The requirement of a notice of copyright was eliminated in 1989 when the U.S. signed the Berne Convention, an international copyright treaty.
[8] *Ty, Inc. v. GMA Accessories, Inc.,* 132 F.3d 1167 (7th Cir. 1997).
[9] *Computer Associates International, Inc., v. Altai, Inc.,* 982 F.2d 693 (2nd Cir. 1992).
[10] *Id.*
[11] See, e.g. *Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.,* 797 F.2d 1222 (3rd Cir. 1986).
[12] Patent Act of 1952, 35 U.S.C. Sec. 101-112 (1952)..
[13] *Id.,* Sec. 101-103.
[14] *Id.,* Sec. 101.
[15] *Gottschalk v. Benson*, 409 U.S. 63 (1972).
[16] *Diamond v. Diehr*, 450 U.S. 175 (1981).
[17] J. William Gurley, *The trouble With Internet Patents,* FORTUNE (July 19, 1999).
[18] *Amazon.com, Inc. v. Barnesandnoble.com, LLC.,* 73 F. Supp.2d 1228 (1999).
[19] William Bulkeley, *Patent Application Could Evolve Into Trouble for E-Commerce,* WALL ST. JOURNAL INTERACTIVE (Aug. 28, 2000).
[20] *Amazon.com, Inc. v. Barnesandnoble.com, LLC,* ___F.3d___, Case # 00-1109 (Fed. Cir. Feb. 14, 2001).
[21] Carol King, *Court Hands Barnesandnoble.com A Legal Victory,* E-COMMERCE NEWS (Feb. 14, 2001).
[22] *Id.*
[23] Scott Thurm, *The Ultimate Weapon,* WALL ST. JOURNAL INTERACTIVE (April 17, 2000).
[24] Federal Trademark Act, 15 U.S.C. 1051-1127 (1988).
[25] GERALD FERRERA, STEPHEN LICHTENSTEIN, MARGO RADER, RAY AUGUST AND WILLIAM SCHIANO, CYBERLAW TEXT AND CASES (2001).
[26] *Playboy Enterprises, Inc. v. Terri Welles, Inc.,* 78 F. Supp.2d 1066 (1999).
[27] PETER MAGGS, JOHN SOMA AND JAMES SPROWL, INTERNTET AND COMPUTER LAW (2001).
[28] *Supra,* note 26.
[29] *Dr. Seuss Enterprises V. Penguin Books USA, Inc.,* 109 F.3d 1394 (9th Cir. 1997).
[30] *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036 (9th Cir. 1999).
[31] MARK RADCLIFFE, THE MULTIMEDIA LAW & BUSINESS HANDBOOK (1999)
[32] *Qualitex Co. v. Jacobson Products Co.,* 115 S. Ct. 1300, (1995). This U. S. Supreme Court case held that a unique color could constitute a valid trademark.
[33] Scott Carver, John McGregor, Min Wu, Adam Stubblefield, Ben Swartzlander, Dan Wallach, Drew Dean, Edward Felten, *Reading Between the Lines: Lessons from the SDMI Challenge,* WIRED (July 2001); excerpted portions. See complete text at cryptome.org/sdmi-attack. This paper was to be presented at the Spring meeting of the Information Hiding Workshop in Pittsburgh, but was withdrawn after threat of litigation from the Recording Industry Association of America.
[34] Uniform Trade Secrets Act, 14 U.L.A. 433 (1990). This Act has been adopted by 40 states.
[35] *Id.* Sec. 4.
[36] *Vermont Microsystems Inc. v. Autodesk, Inc.,* 88 F.3d 142 (2nd Cir. 1996).
[37] *Ed Nowogroski Insurance, Inc. v. Rucker,* 971 P.2d 936 (Wa. S. Ct. 1999).
[38] *Brunswick Floors, Inc. v. Guest,* 506 S.E.2d 670 (Ct. App. Ga. 1998).
[39] RICHARD MANN & BARRY ROBERTS, SMITH AND ROBERSON'S BUSINESS LAW (11th ed. 2000).
[40] *Id.*
[41] *Id.*
[42] *Smith v. Pillsbury*, 914 F.Supp. 97 (E.D. Pa. 1996).
[43] *U.S. v. Simons*, ___F.3d___ 2000 WL 223332, (4th Cir. 2000).
[44] Carl Kaplan, *Reconsidering the Privacy of Office Computers,* THE NEW YORK TIMES (July 27, 2001).
[45] Bob Dylan, *Like a Rolling Stone* (1965).
[46] NATIONAL DISTRICT ATTORNEYS ASSOCIATION, THE PROSECUTOR'S DESKBOOK 13 (1971).
[47] Economic Espionage Act of 1996, 18 U.S.C. 1831-1839 (1996).
[48] No Electronic Theft Act of 1997, 17 U.S.C. 505 and 18 U.S.C. 2319 (1997).
[49] 18 U.S.C. Sec. 1030 (1999).

[50] 18 U.S.C. Sec. 1030(e)(2)(B) (1999).
[51] David Gallagher, *Invisible Publishing Sparks a Lawsuit*, THE NEW YORK TIMES (June 29, 2001).
[52] HENRY CHEESEMAN, BUSINESS LAW 327 (4th Ed. 2001).
[53] Alan Farnham, *How Safe Are Your Secrets?*, FORTUNE (Sept. 8, 1997).
[54] The New York Times, *High Bail Is Ordered In Trade-Secret Case*, THE NEW YORK TIMES (May 15, 2001).

â€œMy legal team are confident that the Supreme Court will hear the appeal given there are such significant legal issues at stake,â€ Dotcom said in a statement. U.S. authorities say Dotcom and three co-accused Megaupload executives cost film studios and record companies more than $500 million and generated more than $175 million in revenue by encouraging paying users to store and share copyrighted material. The Court of Appeal said the United States had disclosed â€œa clear prima facie case that the appellants conspired to, and did, breach copyright wilfully and on a large scale, for their commerci