Conceal or Perish?

An Overview of Trade Secrets and the Software Industry

Louise Giam & Albert Leung
Fall 2004
6.901 Inventions and Patents
Robert Rines

Background and History

While the value of knowledge and information has been recognized throughout history, the practice of freely disclosing and sharing information is relatively young. Instead, history has favored an approach of hiding invention and discovery so that the benefits of such innovations are not extended beyond a scope defined by some overseeing authority. Even as our founding fathers first conceived the framework which would eventually provide patent rights and protection, the States were already engaged in maneuvers to steal technology secrets that Britain was holding to its competitive advantage. In his "Report on Manufactures," Alexander Hamilton emphasized the need to promote emigration in an effort to bring not only the most talented individuals, but the secret knowledge they might possess, to the States[1], but this general attitude often manifested in ways less subtle than Hamilton's writings. During the 1790s, Thomas Attwood Digges and other Americans engaged in aggressive technology piracy, encouraged by Hamilton and others in the government, which would bring such inventions as the double loom across the Atlantic. In fact, the section of the Constitution used today to champion inventors' rights and patents was initially interpreted as "a mandate to use the mechanism of the new national government effectively to appropriate forbidden European technology"[2]. Eventually, these practices were suppressed to maintain consistency in the principles of the State, but they demonstrate that even a nation with as strong notions of property and patent rights as our own can have a history of involvement with trade secrets.

The history of trade secrets dwarfs the history of patents, and the practice of nondisclosure continues even well after patent systems have been established. The theft of British technologies by Americans continued into the later history of this country; to cite another example, a Harvard businessman effectively stole yet another British loom, the Bridport Loom, in 1811. However, the Americans were by no means the pioneers of such theft, nor were the British strictly its victims. The origins of the British patent system were not unlike those of its American counterpart, with patent rights originally offered as bait to lure in manufacturers with expert secret knowledge. The first documented case of trade secret theft occurred as early as the fifth century, when Byzantine emperor Justinian arranged for two monks to smuggle silkworm eggs from the Far East to attempt to break China's dominance of the silk market[3].

Outside of international competition, trade secrets have been an integral part of business and industry since the dawn of civilization. The notion of a trade as an occupation or role has always involved some expert knowledge that put the tradesman at a comparative advantage to others, affording efficiencies that benefited both the tradesman and society as a whole. Often times, this expert knowledge was also secret knowledge—techniques, formulas, or recipes developed over time and passed from generation to generation, parent to child, master to apprentice. The exclusiveness of this secret knowledge allowed skilled laborers to profit from their practices and continue to develop their abilities without interference of cheap competition. This underlying principle was behind many business and occupation models throughout history, including healers in tribal societies and the trade guilds of the Medieval era.

In modern times, trade secrets form the cornerstone of many businesses where other approaches do not provide sufficient safeguards to the intangible assets of greatest value. One famous example is that of Coca Cola, whose hundred-year-old recipe known as "Merchandise 7X" is

[1] A. Hamilton, "Report on Manufactures," The Papers of Alexander Hamilton, ed. Harold C Syrett et al. (New York: Columbia UP, 1961) 252-256.

[2] D. Ben-Atar, "A U.S Technology Double Standard?," The Globalist 20 Oct. 2004.

[3] L. Bilton, "I've Got a Secret!: Trade Secrets and Industrial Espionage in the Talking Machine Industry" Apr. 2004 <http://www.intertique.com/GotASecret.htm>

one of the best kept secrets of today, with only two individuals allowed to possess this knowledge at any time[4]. Other examples exist in the software industry, where companies are faced with a combination of three separate systems of intellectual property protection. It has been seen that companies often choose to keep secret the actual algorithms and code that allows their products to function while revealing only what is necessary for the product to sell.

What Is A Trade Secret?

We all have an intuition about what a trade secret is, and the formal definition does not differ much from intuition. Trade secrets are broad pieces of information or knowledge that are not generally known, hold economic value, and whose secrecy is actively protected. The first criterion is comparable to a patent's requirement of non-obviousness; public knowledge is never classifiable as a trade secret, regardless of the efforts made to protect it. The second criterion is comparable to the notion of usefulness in patents, maintaining that there must be an economic incentive for the legal protection of the information's secrecy. The third criterion is comparable to the diligence requirement in patent cases; it must be shown that an entity diligently acted to protect its trade secret, just as an inventor must work diligently at developing his invention, in order to receive favorable protection under the law. Other similarities include the status of trade secret rights as negative equitable rights, where violations (also termed "misappropriations") may be litigated, rather than property rights, which are rights to use or own.

The Laws of Trade Secrets

Among the first legal acknowledgements of trade secrets in the United States was through Section 757 of the First Restatement of Torts in 1939. This section made explicit provisions for trade secret protection, including formalized definitions of trade secrets and misappropriations. According to the restatement, a trade secret could be "a formula for a chemical compound, a process of manufacturing, treating, or preserving materials, a pattern for a machine or other device, or a list of customers," sharing many of the categories of things patentable. The restatement also defines the conditions under which a trade secret has been inappropriately taken. In addition, the restatement lists factors that should be considered when deciding whether knowledge is a trade secret, including:

1. the extent to which the information is known outside of his business;
2. the extent to which it is known by employees and others involved in his business;
3. the extent of measures taken by him to guard the secrecy of the information;
4. the value of the information to him and to his competitors;
5. the amount of effort or money expended by him in developing the information;
6. the ease or difficulty with which the information could be properly acquired or duplicated by others[5]

While the First Restatement of Torts seemed to provide a formal understanding of trade secrets and the related litigation, the restatement was by no means the law of the land, and actual trade secret law was left to the discretion of the states. As a result, the development of trade secret law was uneven, with more litigation in large commercial states than agricultural ones. Further complication arose when the Second Restatement of Torts was released in 1978, eliminating the

[4] T. J. Franklin, "Safeguarding Your Business's Trade Secrets," Corporate Logo Dec. 2004 <http://www.corporatelogo.com/articles/441branding.html>

[5] *Restatement of Torts*, §757

definition of trade secrets that had before at least served as a common point of reference. Fortunately, a new standard was soon to be developed in the Uniform Trade Secrets Act.

The Uniform Trade Secrets Act of 1985 set forth a refined definition of trade secrets and called for broad state adoption. Under this new act, the definition of a trade secret covered all the same classes of knowledge as in the original Restatement, but further elaborated the criteria to allow for trade secrets that have yet to be put to use, and also secrets with negative value. In addition, the UTSA expanded on the definition of misappropriation, so that both the act of improperly disclosing and the act of improperly obtaining trade secrets were subject to liability. Finally, the act set forth the terms of relief, with a statute of limitations of three years and permission for both injunctions and recovery of damages. Forty three states have adopted the act or their own customized version, and the remaining seven provide for trade secret protection in their own common law.

Even with the Uniform Trade Secrets Act so widely adopted, there were still significant discrepancies between the handling of trade secrets in the many state courts, and so the federal government took steps to correct this through the Economic Espionage Act of 1996. In this act, the definition of a trade secret was once again broadened to ignore the medium through which theft might occur, whether photographic, electronic, human memory, or otherwise. In addition, violation of trade secrets became punishable by both civil and criminal means. In recent years, there have been several cases exercising the penalties set forth in this act, with defendants facing prison sentences as great as twenty years and fines as much as a quarter million dollars.[6]

Trade Secrets vs. Patents

Despite the similarities in what makes it possible to protect information as trade secrets or through patents, many differences remain to distinguish the two classes of intellectual property. Most notably, the contract of the patent, and indeed the very root of the term, requires disclosure of an invention by its inventor in exchange for limited exclusive rights. In contrast, no such disclosure is required for a trade secret, and instead, non-disclosure is necessary to demonstrate a trade secret's integrity. Part of a patent's contract of limited rights is an expiration date after which the patent is no longer valid. Trade secrets, on the other hand, can be maintained for as long as they meet the definition of being a trade secret. In addition, while patents are held by a single party, the trade secret rights to any information may simultaneously be held by multiple parties. Overall, the courts have provided good insight into the rationale behind these distinctions:

> Quite clearly discovery is something less than invention. Invention requires genius, imagination, inspiration, or whatever is the faculty that gives birth to the inventive concept. Discovery may be the result of industry, application, or be perhaps merely fortuitous. The discoverer, however, is entitled to the same protection as the inventor.
>
> The mere fact that the means by which a discovery is made are obvious, that experimentation which leads from known factors to an ascertainable but presently unknown result may be simple, we think cannot destroy the value of the discovery to one who makes it, or advantage the competitor by unfair means, or as the beneficiary of a broken faith, obtains the desired knowledge without himself paying the price in labor, money, or machines expended by the discoverer. Facts of great value may, like the lost purse upon the highway, lie long unnoticed upon the public commons. Hundreds pass them by, till one more observant than the rest makes discovery. It is idle to say that, in the eyes of the law, interest may not in such case follow discernment[7].

Patents also differ from trade secrets in the process to obtain and breadth of coverage. When filing a patent, carefully worded claims must describe the invention. It is possible to find a

[6] E. Linek, "A Brief History of Trade Secret Law," BioProcess International Nov. 2004 2(10):20-26

[7] *A. O. Smith Corp.* v. *Petroleum Iron Works Co.* (Sixth Circuit Court of Appeals 1934) 73 F.2d 531.

dominating patent that has encompassed what you have described, thereby preventing the use of your technology without licensing. On the other hand, if the patent is granted, the government has approved the technology within the scope of the claims. It is possible that the scope of the claims is much smaller than what actually describes the invention and therefore the idea is not fully protected with just a patent. Conversely, trade secrets can be broad because they are defined by vague concepts of usefulness. Trade secrets tread on much larger ground and unlike patents, the process of describing and categorizing a trade secret is not required by law.

Securing a patent is an expensive and slow process with an average wait time of at least a year (and nowadays, closer to three). Even when the patent has been issued, enforcing it may be costly as well because of litigation against infringers or uncooperative licensees. Monitoring patent infringement is extremely difficult because it may be possible to never discover its occurrence if the infringer is smart and careful. While trade secrets are not subject to the same slow approval process, protecting trade secrets is not necessarily less expensive because of security measures a company must take to protect their intellectual property.

When it comes to defending intellectual property rights, the patent provides stronger protection against a competitor's use of one's ideas. Beyond proving infringement, the defense of a patent only involves proof of validity; patents run the risk of courts invalidating them or citing infringements on prior art. If these matters can be proven, the patent will offer complete exclusive rights against unlicensed commercial use until expiration. Trade secrets, however, are only defended against parties who obtain them unfairly, as in those who violate confidential agreements or engage in industrial espionage. These measures are more difficult to prove than infringement, as it provides for various methods of uncovering a trade secret that are legal, including reverse engineering or independent discovery. It is only possible to guess when and whether someone else will make the discovery, and if he will keep it confidential or disclose the secret.

The issue of defense reveals a significant vulnerability in trade secrets: it is impossible to protect against the usage of a trade secret if access to this secret has been obtained lawfully. Reverse engineering, or working backwards to determine materials, methods, and designs, is under most circumstances, perfectly legal and acceptable. It is not considered to be an improper means of gaining access to secret information because the release of an invention or product into the public domain for sale openly exposes aspects that may be enough to allow the trade secrets to be discovered. If it should happen that an examination of a product reveals secrets of its composition, then the intellectual property can no longer be protected. It is not permitted, however, for a party to reverse engineer and duplicate a patented invention, as decided by the courts:

> It is well recognized that a trade secret does not offer protection against discovery by fair and honest means such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is, starting with the known product and working backward to divine the process. Thus, it is the employment of improper means to procure the trade secret, rather than mere copying or use, which is the basis of liability[8].

Many factors influence the choice between patent protection and trade secret protection. A fundamental part of protecting intellectual property is to profit from selling or licensing the technology. Patent licensing is often easier than trade secret licensing because there are well-defined procedures governing it. Because trade secrets by their very nature are ambiguous, applying terms for licensing become blurred since there is no government-issued approval. Furthermore, licensing a trade secret also entails policing the licensee's measures for protecting the trade secret against disclosure and can become a hassle.

[8] *Chicago Lock Co.* v. *Fanberg* (Ninth Circuit Court of Appeals 1982) 676 F.2d 400.

In most cases, the nature of the knowledge itself dictates which form of protection is taken. For example, patent protection is usually inappropriate for some company know-how or lesser tricks.

The finer differences between patent and trade secret protection are seen in the early stages of actually seeking intellectual property protection. It is possible to apply for a patent while keeping the trade secret status of an idea. These measures safeguard the idea in the event that the patent is rejected because the trade secret status of the idea remains. Though patents require thorough descriptions of an invention, it is still common to maintain trade secrets related to the patent. It is a fine line between the requisite disclosures of the "best mode" of invention while holding back trade secret information applicable to the patent, which may later be invalidated due to lack of specificity.

Trade Secrets vs. Copyrights

Unlike a patent, a copyright is relatively simple and easy to obtain. Copyright laws only protect the *expression* of an idea, which differs from trade secret protection, which can extend to anything pertaining to the idea. The author's work need only be "original" and fixed in a tangible medium of expression to receive copyright protection, whereas an invention must be new, useful, and non-obvious to be considered for patent protection. That the work was created by the author and involved a "modicum" of creativity is the only requirement necessary for copyright law. Works are copyright protected as soon as they are fixed in a tangible medium of expression and no registration is required, though there are advantages for registration.

Copyright law governs an author's reproduction and distribution rights, which are separate and distinct. The author is, secondly, given exclusive rights to creating derivative works based upon that initial copyrighted work. Lastly, the author can control the public performance and display of the copyrighted work. Works created after January 1, 1978 have copyrights that last until seventy years after the author's death. For anonymous works owned by companies, the copyright lasts for ninety-five years from the first publication of the work, or one hundred years from the work's creation, whichever occurs first.

As with the debate of choosing between patent and trade secret, the nature of the idea governs the mode of protection. Some inventions must be widely published or distributed in order to make money and in this case, it is often advisable to use copyrights. Just as in the software industry, where a significant investment has been made and extensive distribution is required, the product is always exposed to the possibility of illegal copying. It follows that the primary mode of protection is the copyright registration in this scenario.

Trade secrets, on the other hand, are clearly the most general and flexible means of protecting intellectual property as compared to the two main statutory forms (patent and copyright). Depending on the method of managing assets and inventions, however, the other methods may prove to be more advantageous and useful.

Trade Secrets and Employee-Employer Relations

As frequently as one encounters assignment of invention agreements in the working world, one will also undoubtedly encounter nondisclosure agreements. While these agreements do serve the purpose of protecting an employer's interests in its intellectual property rights, they do so in a slightly different manner than assignments of invention. Unlike the case of patents, where businesses actively attempt to wrest inventions from the hands of their employees, it is a matter of law that these nondisclosure agreements are used; only if a business practices strict policies guarding its trade secrets will these secrets be defensible under the law. Included in these policies are the familiar nondisclosure agreements, as well as physical security measures like locks and passwords and other strict controls over secret information.

Despite clear and explicit intentions in law to protect trade secrets, the courts have often ruled in favor of employee rights, and there remains a sensitive balance between what is protected for the employee and the employer in working relationships. The courts "recognize and actively protect the right of employees to carry away and use general skills or knowledge brought by them to a job or acquired during the course of employment,"[9] and this knowledge may even include trade secrets. However, were employees to agree to nondisclosure as part of their contracts of employment, they will have waived rights that the courts would otherwise be willing to defend. This is similar to the nature of invention and the workplace: by law alone, an employer has little claim to the innovations of the employee, but these rights are often exchanged as a part of the employment agreement. The critical difference, as mentioned above, is that employers may be more insistent with nondisclosure, since failure in doing so may undermine the validity of all trade secrets that are a part of the business' operation.

Even if an employee has signed a nondisclosure agreement, the employee still has an opportunity to gain some rights to the trade secrets of the employ since trade secrets are not limited to a single holder. This situation precisely describes the instance when an employee has played some instrumental role in the development of the trade secret. Under the Milton Bradley doctrine[10], the employee has limited rights to benefit from trade secrets that he has helped to develop; the courts have ruled that the role of developer gives the employee "an unqualified privilege to use and disclose the trade secrets so developed"[11]. This again reflects the attitude that workers are allowed and expected to gain technical skill during the course of their employment.

Trade Secrets and the Software Industry

With some background on the definition, legal protection, and practice of trade secrets, we now consider their applications to a specific industry, the software industry. This industry is of particular interest because the nature of software goods requires strong intellectual property rights. As intangible goods, software products are very cheap to mass produce and replicate without significant investment into process, machines, or materials. The value of software is entirely contained in the ideas and methods that the software captures. With such an abstract source of value, only protection of the knowledge or invention itself can be used to safeguard the assets of a software business.

As it turns out, all three of the major classes of intellectual property protection are applicable to software. The copyright was the traditional medium for safeguarding software and the code that made it work, but with the first approval of software patents in the 1980s, the use of patents by the industry has grown substantially. Trade secrets also form a large part of the industry's protection scheme, and the underlying mechanisms behind many software products remain secret and valuable knowledge of the companies in the industry. Because of the concurrent use of all these modes of protection, we can compare the effectiveness of these modes in practice and observe how they are used in relation to each other.

Trade Secrets: A Natural Choice?

With the non-physical nature of software comes unwillingness among developers to disclose any significant amount of information about the inner workings of their software, since doing so will

[9] L. T. Gesmer, "Trade Secret Protection of Computer Software," Trade Secret Law Reporter Jan. 1986.
[10] *New Method Die & Cut-Out Co. v. Milton Bradley Co.*, 289 Mass. 277,289-90 (1935).
[11] *Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp.*, (E.D. Mich. 1975) 401 F. Supp. 1110-12.

likely allow others to steal or mimic the ideas. Consequently, one would expect that the natural choice for software protection would be the trade secret, where disclosure or even registration is unnecessary. Historically, this may have been the case, with the mere secrecy of the source code behind software enough a defense from the competition. However, as computer technical skills became more common, the vulnerability of the trade secret to both independent discovery and reverse engineering became a considerable threat. Trade secrets alone became insufficient protection and software firms looked to other means.

Copyright Protection for Software: Whelan Associates v. *Jaslow Dental Laboratories*

The next choice for securing software became the copyright. Unfortunately, copyright protection initially extended only to the *expression of an idea*—essentially, protecting the code from being literally copied, line for line. It is, however, equally important to be able to protect non-literal elements of a software program, such as its structure, sequence, and organization.
A pivotal court ruling would extend the coverage of copyrights, allowing their effective use for software.

In 1978, Rand Jaslow, who had no programming experience, tried writing a computer program to deal with billing, accounting, inventory, and other business operations at Jaslow Dental Laboratory. Without success, he hired Strohl Systems to develop the software for $18,000 on an IBM Series 1 computer. In their agreement, Strohl "retained ownership of the software and could market it to other dental laboratories"[12]. Through the agreement, Jaslow Laboratories would also be able to collect a ten percent royalty on the software sales.

Elaine Whelan, a half-owner of Strohl, designed the software and completed it in March 1979. She then left in November of that same year to form her own company, Whelan Associates, Inc. The company formed an agreement with Jaslow Laboratories allowing Jaslow to be the exclusive sales representative for the software, marketed under the name Dentalab, in exchange for "35 percent of the gross sales price and 5 percent of any modification work"[13].

For two years, the two parties got along decently well, but Jaslow then sought to create a new version of Dentalab for smaller personal computers using the BASIC programming language. Jaslow gained access to the Dentalab source code without the consent of Whelan or Strohl and this new version closely copied the functionality and interfaces of Dentalab. As Jaslow's version was nearing its final stages of development, the company terminated its contract with Whelan. They also alleged that the Dentalab software contained valuable trade secrets, suggesting that Whelan should discontinue sales.

Jaslow then formed a new company, Dentcom, to market the IBM-PC version of the software, Dentlab. Dentcom then sold to twenty-three customers, earning gross profits of more than $100,000. On June 30, 1983, Jaslow filed a lawsuit in the state court of Pennsylvania, alleging that Whelan Associates had "misappropriated its trade secrets." Whelan Associates responded by filing a lawsuit in the federal court of Pennsylvania, saying that [the Dentlab software infringed copyrights in the Dentalab software.]

The court ruled for Whelan Associates on all counts because Dentcom's version of the software contained "nearly identical file structures and screen displays"[14] and awarded damages to Whelan in an amount equal to Dentcom's profits from Dentlab and forbade Dentcom from any further sales of the copied version of Dentlab.

[12] Graham, Lawrence. *Legal Battles that Shaped the Computer Industry.* Quorum Books. Westport, USA. 1999.

[13] *Whelan Associates* v. *Jaslow Dental Laboratories, Inc.* (District Court of Pennsylvania 1985) 609 F. Supp. 1307.

[14] *Whelan Associates* v. *Jaslow Dental Laboratories, Inc.* (District Court of Pennsylvania 1985) 609 F. Supp. 1325.

Dentcom appealed the decision to the U.S. Court of Appeals for the Third Circuit, which upheld the decision of the trial court. They applied that the "idea" of Dentalab was a program that would automate dental laboratory business functions, while the "expression" was what the software did to carry out this idea:

> Copyrights do not protect ideas – only expressions of ideas. There are many ways that the same data may be organized, assembled, held, retrieved and utilized by a computer. *Different computer systems may functionally serve similar purposes without being copies of each other. There is evidence in the record that there are other software programs for the business management of dental laboratories in competition with plaintiff's program. There is no contention that any of them infringe although they may incorporate many of the same ideas and functions.* The 'expression of the idea' in a software computer program is the manner in which the program operates, controls and regulates the computer in receiving, assembling, calculating, retaining, correlating, and producing information either on a screen, print-out or by audio communication.[15]

The decision deliberated by the appelate court extended copyright protection to functional aspects of software, thereby extending protection to beyond the program's literal code to include structure, sequence, and organization. The *Whelan* decision set a precedent that a company's software would enjoy broad rights under copyright law. It would therefore be difficult to develop software after seeing another program's source code without infringing on its copyrights. This case encourages and ensures that competing software is developed independently and without access to source code for direct copying.

The *Whelan* case and other similar holdings strengthened the protection given to software by copyrights. Through copyrights, companies were given a legal device to protect not only the literal embodiment but also the functional structure of their software. Copyrights would also afford some protection against reverse engineering that was lacking in the use of trade secrets. However, while the courts have chosen this interpretation and usage of copyright law, it is unclear that the original intent of copyrights included such a function and that copyrights are indeed the appropriate mechanism for software protection.

Software Patents: In re Alappat

The next breakthrough for the defense of software intellectual property came with the allowance of software patents. For many years, it was not possible to apply for a software patent because the general view was that software fell under the class of algorithms, mathematical or otherwise, and algorithms, as parts of the fundamental order of nature, could not be patented. This attitude was exemplified when the Supreme Court ruled in favor of the U.S. Patent and Trademark Office, upholding the rejection of a patent application claiming "an invention in a software algorithm for converting numbers in binary-coded decimal format to binary format"[16].

This perspective of software as a fundamental natural algorithm would reverse as the courts began to consider the hardware implementations that were coupled with software. In a landmark case for software patents, Kuriappan Alappat, Edward Ayerill, and James Larsen jointly invented and attempted to patent a rasterizer for a digital oscilloscope. The rasterizer would reduce the effect of jagged pixels in the displayed waveforms by a method that involved modifying the pixels lying close to the desired waveform,causing them to appear dimmer. The invention claims:

> a rasterizer for converting vector list data representing sample magnitudes of an input waveform into anti-aliased pixel illumination intensity data to be displayed on a display means comprising:

[15] *Whelan Associates* v. *Jaslow Dental Laboratories, Inc.* (Third Circuit Court of Appeals 1986) 797 F.2d 1222.
[16] *Gottschalk* v. *Benson* (Supreme Court 1972) 409 U.S. 63.

> (a) means for determining the vertical distance between the endpoints of the vectors in the data list;
> (b) means for determining the elevation of a row of pixels that is spanned by the vector;
> (c) means for normalizing the distance and elevation; and
> (d) means for outputting illumination intensity data as a predetermined function of the normalized vertical distance and elevation[17].

The U.S. Patent Office and the Board of Patent Appeals and Interferences rejected the application because the claimed invention was in actuality a mathematical algorithm, and therefore not patentable.

The Federal Circuit Court of Appeals, however, reversed the decision of the Patent Office and decided that the "means for" elements in the patent were for physical components rather than mathematical algorithms. The Alappat application had examples of electronic circuit elements that would perform the steps that were claimed and thus, as a machine, as opposed to mathematical formulae, could be patented. The court set a precedent that even if Alappat's invention were a software algorithm, it would still warrant patent protection:

> We have held that such programming creates a new machine, because a general purpose computer in effect becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software[18].

The *In re Alappat* decision resolved the question surrounding the patentability of software inventions. The focus instead turned to whether an invention claims a *patentable application* of mathematical algorithms rather than the *unpatentable algorithm* itself. Interestingly enough, the number of software-related patent applications tripled from 1988 to 1994, the year *Alappat* was decided. After the confirmation of software patentability, more companies and groups sought to protect their inventions through patents.

The few companies that patented their software early on had a slight advantage over those who did not have the notion to protect their intellectual property. The software companies with a strong patent culture can rest assured that the courts will not invalidate their patents on the mere basis of their invention being computer software. As a matter of defensive strategy, companies are able to protect their investments by precluding others from reverse engineering patented software. This precedent is extremely valuable to software companies because it forces other parties to take out licenses. The software patent ensures the inventor the right to prevent others from making, using, or selling the invention and is a powerful safeguard against the replication and distribution of a patented product.

Shrink-wrap Licensing: ProCD, Inc. v. *Zeidenberg*

In the 1990s, the courts approved the validity of another mechanism for software protection, the use of compulsory licensing by end-users. These so-called "shrink-wrap" licenses are integrated into the packaging of software and must be accepted by consumers as contracts of use. They often prohibit the production, copying, rental, and reverse engineering of software, and restrict software to be used on a single computer. Through these licenses, companies have been able to extend the effectiveness of their trade secrets by preventing direct reverse engineering of their commercially released products. In order to access these products, an individual would have to agree to the license, thereby relinquishing any rights he would otherwise have to reverse engineer the products.

[17] Alappat, Kuriappan, *et al.* Raster scan waveform display rasterizer with pixel intensity gradation, assignee. Patent 5,440,676. 8 Aug. 1995.

[18] *In re Alappat* (Federal Circuit Court 1994) 33 F.3d 1526.

Shrink-wrap licenses, however, raise the issue of enforceability because consumers are not able to review the terms of the license before the purchase. Because of the questionability of enforceability, few software makers have sought to enforce the shrink-wrap license in court. The licenses have also made their way instead to "splash screens" that require the users to consent to terms in the license before the software will install.

Generally, shrink-wrap licenses have been looked upon by courts with disapproval. No court had addressed the enforceability of these shrink-wrap licenses until the dispute between ProCD, Inc. and Matthew Zeidenberg in 1996.

ProCD, Inc. spent more than $10 million developing and maintaining a national telephone and address database that included residential and commercial listings. They produced this database in several formats including a CD-ROM, which was marketed as a software program called Select Phone. Like other software, it had a reference in fine print on the outside of the box and license documentation inside requesting consumers to review the terms before using it. There was also a splash screen agreement that the consumer needed to agree to before using the software. ProCD chose these measures because it recognized that if others could freely distribute their software, then they would not be able to recover their investments. Part of the agreement included a provision that prohibited purchasers from making the software available to others over any network.

In 1994 Matthew Zeidenberg bought a copy of Select Phone and then decided in early 1995 to use the data in it to make a commercial directory accessible through the Internet. In March 1995 he purchased an updated version of Select Phone for his directory and he formed his own company, Silken Mountain Web Services, Inc. He wrote his own program to search through the database and the directory became popular, receiving around 20,000 visits per day. ProCD discovered the Silken Mountain database and demanded that it be removed. Although Zeidenberg admitted to having used listings from Select Phone, he refused to remove his program because he did not believe the licenses in Select Phone to be binding.

In September 1995, ProCD sued Zeidenberg and Silken Mountain, seeking damages for copyright infringement, breach of the shrink-wrap license agreement, and violation of the Wisconsin State Computer Crimes Act. The court needed to address whether the data *could* be protected by copyright and whether the shrink-wrap license was valid and *enforceable*. To this end, the court noted that ProCD obtained its data in much the same way as Zeidenberg through the use of phone books that were created by others.

The trial court then concluded that the shrink-wrap license was not enforceable because Zeidenberg did not have the chance to review the terms of agreement before purchasing the software. It did not matter that he bought two copies because the court said there was no possibility of knowing whether the agreement remained the same between the different versions. Because there was no opportunity to review the license, it was not enforceable under the Uniform Commercial Code (UCC), a broad set of laws governing the sale of goods [19].

ProCD appealed the decision and the Seventh Circuit Court reversed the decision, ruling that shrink-wrap licenses were indeed enforceable. Because there was a notice on the outside of the box informing the consumer that there was a license inside, Zeidenberg understood his purchase would entail a licensing agreement. If he did not agree with the terms proscribed, he could have returned the software. Zeidenberg was given the option of reviewing and rejecting the license before agreeing to them in the splash screen as well.

The Court of Appeals said that having the notice on the outside with the terms on the inside made logical sense for doing business. It would be impractical to reproduce the entire agreement

[19] *ProCD, Inc.* v. *Zeidenberg* (W.D. Wis. 1996) 908 F. Supp. 640.

common but as individuals, do not have much capacity to pay damages. Ultimately the mode of intellectual property protection is governed by the software product and the desire to profit from investments. The software program is in itself a difficult invention to protect because of many avenues that cause the inventor to lose his competitive advantage including reverse engineering, the circumvention of law other parties use in copying software illegally, and many other methods. While the rights of software may be well established, the means of enforcing these rights still need to be developed further. Here there are no options!