FENWICK & WEST LLP

Intellectual Property Bulletin

Fenwick & West LLP — Fall 1997

FENWICK & WEST LLP

About The Firm

Fenwick & West LLP provides comprehensive legal services to high technology and life sciences clients of national and international prominence. We have over 280 attorneys and a network of correspondent firms in many major cities throughout the world. We have offices in Mountain View and San Francisco, California and Washington, D.C.

Fenwick is committed to providing excellent, cost-effective and practical legal services and solutions that focus on global high technology industries and issues. We believe that technology will continue to drive our national and global economies, and look forward to partnering with our clients to create the products and services that will help build great companies. We differentiate ourselves by having greater depth in our understanding of our clients' technologies, industry environment and business needs than is typically expected of lawyers.

Fenwick is a full service law firm with "best of breed" practice groups covering:

- Corporate (emerging growth, financings, securities, mergers and acquisitions)
- Intellectual Property (patent, copyright, licensing, trademark)
- Government Contracts and Technology Transfer
- Litigation (commercial and IP litigation)
- Tax

Our Offices

Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel: 650.988.8500
Fax: 650.938.5200

Suite 200
815 Connecticut Avenue NW
Washington, DC 20006
Tel: 202.261.0400
Fax: 202.463.6520

Embarcadero Center West
275 Battery Street
San Francisco, CA 94111
Tel: 415.875.2300
Fax: 415.281.1350

For more information about Fenwick & West LLP, please visit our Website at: www.fenwick.com.

The contents of this publication are not intended, and cannot be considered, as legal advice or opinion.

© 2003, 1997 Fenwick & West LLP. All Rights Reserved.

FENWICK & WEST LLP

Intellectual Property Bulletin

Fall 1997

Table of Contents

Intellectual Property Issues In Eradicating the Millennium Bug

by Tim Alan Covington (tcovington@fenwick.com)

A number of intellectual property issues arise as a result of the "Millennium Bug" or "Year 2000" (also known as "Y2K") problem. Some of them derive from the intellectual property laws themselves. Others derive from contracts concerning intellectual property rights.

The Millennium Bug is generally regarded as a programming attribute that does not allow software to process date data that transcends the Millennium (*i.e.* data containing dates that occur before, on and after the Year 2000). When software and computer systems having the Millennium Bug attempt to process such "trans-Millennnium date data" they can fail to initiate, malfunction or terminate abnormally.

Almost all software distributed worldwide up until the last few years contains the Millennium Bug. Some software distributed even today is not programmed to process trans-Millennium date data. Such software includes computer operating systems, business applications, and firmware or microcode that comprises the intelligence of microcomputers that control most modern electronic equipment and devices. The potentially horrific consequences of massive failure of the world's computer systems at the Millennium has prompted many companies to reprogram their products and systems. Their attempts at reprogramming raise a number of issues, both under intellectual property laws and under contracts governing the licensing and use of computer products and technology.

One of the most obvious intellectual property issues in attempting to eradicate the Millennium Bug arises under the U.S. Copyright Act and similar laws of other countries. The Copyright Act provides a virtual monopoly to the copyright holder on commercial rights to exploit the copyright work of authorship (software is such a work). As a general matter, if the copyright holder does not expressly authorize a commercial right in writing, then the copyright holder retains that right (subject to a weak and recently developed doctrine of implied rights, as discussed below).

Many companies employing "self-help" in reprogramming computer systems they have acquired from others may be exceeding the scope of their rights under a software copyright license. Many software licenses permit use, reproduction, and even sublicensing and distribution. However, such licenses often do not permit modification or the creation of derivative works. In fact, a large number of licenses expressly prohibit such activities as reverse engineering, decompilation, reverse analysis, modification and the creation of derivative works. If a license contains such prohibitions, and the consent of the copyright holder or other authorized person is not obtained in order to modify code, then the

modifications made, whether to allow the processing of trans-Millennium date data or otherwise, may constitute a breach of the license agreement and an infringement of the copyright in the code.

A few courts have held that implied license rights may exist where rights of the copyright holder are not expressly reserved, even though they are not expressly granted. Accordingly, it is possible that some software licensees may have an implied right of self-help in addressing their Y2K issues. However, whether these rights exists under any particular license agreement may depend on a specific interpretation of the language of the agreement, the subject of the agreement, and surrounding facts. The licensee may not be able to determine for sure whether there are implied rights of self-help.

Contacting the licensor for a clarification of implied rights, or to obtain express rights to modify software, may make matters worse, if the licensee must modify its systems in order to avoid catastrophe at the Millennium. The licensor may refuse the request for express rights or clarification, casting further doubt on the existence of an implied right.

These very same issues may exist for distributors of proprietary software who acquire and resell underlying or related software. However, many software distribution licenses do allow for rights to modify software for some purposes, such as to create interfaces or to "integrate" the vendor's software with the distributor's software. Such broad distribution rights may contain rights to modify for other purposes, including Millennium reprogramming.

Many software users do not have the technical expertise or resources for self-help. They hire consultants to fix problems, including the Millennium Bug. Many of these users are unaware that their consultants frequently do not have any greater rights than does the user to modify licensed code. A few such consultants are aware of the potential infringement resulting from such modification and have provided in their service contracts that it is the user's responsibility to obtain consents of software licensors necessary to perform Millennium modifications. If a user agrees to such a provision, then the user, in addition to potential liability for infringement and contributory infringement, may have potential liability to the consultant for breach of contract, if the consents are not actually obtained. Ironically, having hired a technical consultant to manage the reprogramming effort, many users are not cognizant of third party software requiring modification and consents, making it unlikely that consents will be sought or obtained.

Systems distributors of others' software often offer sales and license contracts to their customers that contain intellectual property infringement indemnities to their customers. Such indemnities protect the customers against third party claims that the systems acquired from the distributor infringe a third party's intellectual property (*e.g.* copyright). Under

common forms of such indemnities, the distributor must pay costs and expenses associated with the claim and related legal proceedings, as well as damages agreed to in settlement or awarded in the proceedings. Such amounts, if not limited in the customer contract, can greatly exceed purchase prices and license fees under the contract. If a distributor has modified code from a supplier without that supplier's authorization or consent then, as discussed above, the modified code may be infringing. If the distributor has indemnified its customers, then the distributor will be obligated under the indemnity to bear its customers' liability for damages, costs and expenses as well.

It is worth noting that, even in the absence of an intellectual property indemnity, a distributor may have liability due to the infringement claim, if there is an implied warranty of non-infringement that has not been expressly disclaimed.

Of course, infringement claims of the kind described above would not result if copyright licensors would consent to self-help through modification of their code. However, many do not provide such consent, for a number of reasons. First, many software licensors cannot, or are unwilling to provide ongoing maintenance for their software if their software has been modified. Second, many licensors are themselves offering or considering offering upgrades to their products that address Year 2000 issues. They view demand for Y2K upgrades not as a problem but as a business opportunity. Third, remarkably, some licensors just do not know enough about Y2K issues to realize the nature of the problem and ramifications of a solution. They are afraid of unknown consequences and do not cooperate due to fear.

Issues under other forms of intellectual property also arise with respect to the Millennium Bug. Techniques for reprogramming to process trans-Millennium date data may be patented. Providers of Y2K reprogramming solutions, to users and distributors alike, should be well-versed in intellectual property issues relating to their solutions. If they are, then they should be able to provide "clean," non-infringing solutions.

Trade secrets also may be at issue in implementing Millennium Bug fixes. Some reprogramming techniques may be trade secrets. There may be an obligation to protect trade secrets on the part of someone to whom they are entrusted, or even someone who knows or should know that they are trade secrets, depending on the circumstances under which they are received. Most unwitting users who benefit from another's use of third party trade secrets are unlikely to have trade secret liability, however.

Many companies' Y2K remediation programs include participation of legal counsel to address legal issues under intellectual property rules, among others. Programs that do not include participation of counsel probably should.

Portions of this article first appeared in The Daily Journal.

Suppression and Concealment of Inventions: A Software Vendor's Nightmare Named 102(g)

by Stuart P. Meyer (smeyer@fenwick.com)

As if the intellectual property mazes confronting software developers were not already confusing enough, there is a relatively unexplored area of patent law that seems tailor-made to wreak havoc in the software industry. Section 102(g) of the patent statute allows defendants in infringement actions to invalidate patents where the technology at issue had previously been invented by someone other than the patentee, but only where the prior invention was not abandoned, suppressed or concealed. As discussed below, there is very little guidance available as to whether an invention that is embodied in software marketed under a typical software license has been suppressed or concealed. Thus, software vendors face the very real prospect of being found to infringe patents that claim subject matter they developed years or even decades before such patents were ever filed.

The United States has a "first to invent" patent system that considers the actual inventor to be the only one eligible for patent protection. Thus, many companies that believe their employees to have been the first true inventors of certain innovations have found security in the notion that they need not worry about later comers claiming to have patent rights in those innovations. Under the traditional wisdom, if they are approached by such a second comer claiming to have patent rights, they need merely demonstrate that the second comer was not in fact the first inventor. For many high technology industries, this is a false and very dangerous notion. Although public use of an invention by a first person (for purposes of discussion, "Frances") will generally make it impossible for the invention of a second person ("Sam") to enjoy United States patent protection, there is an important exception to this principle in the patent law: Inventions that are "abandoned, suppressed, or concealed" such as by trade secrecy, cannot be used as "prior art" by Frances to defeat Sam's patent.

Consider that Frances developed an innovative sorting algorithm in 1997 that permits software produced by her company to process data significantly faster than the competitive offerings. If this software is marketed using a traditional restrictive license agreement that characterizes the software as containing Frances' trade secrets and that prevents the end user from decompiling, disassembling, or otherwise disclosing or using trade secrets in the software, it may be successfully argued that Frances' invention has been "suppressed or concealed." Thus, if Sam happens to come up with an identical invention in 1998 and obtains a patent for the invention, Frances may not be able to use her earlier invention as prior art to invalidate the patent on Sam's later invention.

Particularly in the software industry, where products are generally marketed under such restrictive licenses rather than by conventional sales, the problem of suppression or

concealment may arise. Sometimes, but not always, the "on-sale" bar of section 102(b) of the patent statute may come into play and save Frances, if, for instance, she offered her invention for sale more than a year before Sam's patent application is filed. However, for various reasons this section 102(b) bar may also be found not to apply.

In August, 1997, the Federal Circuit observed that, "[T]he patent laws have not generally recognized as prior art that which is not accessible to the public." *OddzOn Products, Inc. v. Just Toys, Inc.*, 122 F.3d 1396 (Fed. Cir. 1997). The court cited as a "basic principle" the notion that prior art is "technology already available to the public." The court further explained that "available" means that the technology is described in the world's accessible literature (including patents), or publicly known or in public use or on sale in this country. Thus, prior art is knowledge that is available, at a given time, to a person of ordinary skill in the art.

Even more specifically on section 102(g), the Federal Circuit noted that the policy of patent law is to permit a subsequent inventor to prevail where a first inventor has not given the public the benefit of the invention due to abandonment without public disclosure, suppression, or concealment. "[W]hen the possessor of secret art (art that has been abandoned, suppressed, or concealed) that predates the critical date is faced with a later-filed patent, the later-filed patent should not be invalidated in the face of this 'prior' art, which has not been made available to the public. Thus, prior, but non-public, inventors yield to later inventors who utilize the patent system."

OddzOn teaches that courts should have little sympathy for those who maintain their inventions in secrecy and then cry foul when a later inventor obtains and enforces patent protection for the same technology.

As one might imagine, draconian enforcement of the public policy enunciated above could have unintended negative effects. For example, should an inventor be penalized for not making available to the public technology that is still under development? Fortunately, the Federal Circuit has taken a reasonable position with respect to such situations, stating that each case needs to be decided on its facts and recognizing that works in progress need not be disclosed. For example, in *Checkpoint Systems, Inc. v. ITC*, 54 F.3d. 756 (Fed. Cir. 1995), the court held that the patent law intentionally penalizes those who do not share with the public the benefit of the knowledge of the invention once the invention has been completed. The court approvingly cited an opinion of its predecessor court for the notion that in order "to negate a finding of suppression or concealment, the public must have gained knowledge of the invention which will insure its preservation in the public domain." However, on the facts in *Checkpoint*, the court held that technology on which a patent application was never filed was not abandoned, suppressed or concealed because the public received "the benefit of the learning" of such technology through commercialization.

The issue of whether commercializing a technology while maintaining it as secret should be viewed as suppression or concealment is of particular interest to software vendors. Since most software is marketed under agreements explicitly stating that the software is a trade secret and must not be disclosed, any unpatented inventions in such software are at least to that extent suppressed and concealed. On the other hand, the public, or at least that segment of the public with which the vendor is willing to enter into a licensing arrangement, is obtaining the benefit of the invention, albeit in an undisclosed manner.

Although some cases suggest that merely commercializing a product is sufficient to show that any invention therein has not been suppressed or concealed, there is enough contrary authority to give any software vendor that does not file a patent application cause for concern. While software vendors provide the public with a benefit by marketing their products, many of the inventions inherent in those products are not disclosed to the licensed end users, much less the public at large.

Unfortunately, the Federal Circuit has declined to provide definitive guidance on this point. An oft-cited Seventh Circuit case pre-dating the establishment of the Federal Circuit holds that "non-informing public uses" are to be distinguished from truly "secret uses" in that the latter represent suppression and concealment while the former do not. *Dunlop Holdings Limited v. Ram Golf Corp.*, 524 F.2d 33 (7th Cir. 1975). Despite the hope of many commentators that this approach be adopted by the Federal Circuit, the Federal Circuit's subsequent decisions on related issues have declined to address, much less adopt, the *Dunlop* analysis.

Until this issue is settled by Congress or the Federal Circuit, software vendors thus should be aware of the risks that attend their decision not to file patent applications for potentially patentable inventions in their software products. Software vendors also should consider the potential downside ramifications of trade secrecy for software, particularly where it seems likely that competitors may independently come up with, and patent, similar technology.

Quick Updates

Federal Circuit Affirms Finding of Willful Infringement Where Opinion Letters Fail to Meet Due Care Standard

In *SRI International, Inc. v. Advanced Technology Laboratories*, 1997 U.S. App. Lexis 29098 (Fed. Cir. 1997), the Federal Circuit affirmed a district court's finding of willful infringement, despite the fact that the defendant had three non-infringement opinion letters from three different attorneys. The Federal Circuit found no clear error in the district court's decision that all three of the opinions failed to meet the standard of due care necessary to serve as exculpatory opinion of counsel. The defendant's in-house patent counsel wrote the first opinion letter and based it on technically inaccurate information. An outside counsel wrote the second opinion letter, finding the patent possibly infringed but invalid in view of a

reference that the plaintiff had earlier submitted to the patent office with a reexamination request. The outside counsel merely restated the Examiner's arguments, which had been resolved in the plaintiff's favor during the reexamination. The defendant's legal vice-president wrote the third opinion letter, finding the patent invalid in view of the same reference relied upon in the second opinion letter and in view of another reference, which the Examiner had found to be non-anticipating and in a non-analogous art during the reexamination. The Federal Circuit could not discern any error in the district court's finding that the defendant could not reasonably rely on these opinion letters.

In addition, the Federal Circuit noted that the defendant knew about the patents during the development of the infringing device, but did not seek advice of counsel until afterwards. The court stated, "[p]rudent behavior generally requires that competent legal advice [be] obtained before the commencement of the infringing activity."

Revival of Unintentionally Abandoned Patent Applications

The Patent and Trademark Office (PTO) has eliminated the one year time limit for filing a petition to revive an unintentionally abandoned application. However, the entire delay, from the date of abandonment to the filing date of the petition to revive, must be unintentional. The rule change is retroactive, but the PTO does not consider a delay to be unintentional if an applicant did not file a petition earlier because the applicant did not believe the old rule would permit revival of the application.

Infringing Invisible Markers Not Permitted On Web Site

In a case of first impression involving trademark rights and the Internet, a federal court in California preliminarily has enjoined a website operator from using another's trademarks as invisible markers to lure business to defendant's site. The dispute in *Playboy Enterprises Inc. v. Calvin Designer Label*, 44 U.S.P.Q. 2d (BNA) 1157 (N.D. Cal. 1997) centered on the search capability developed by Internet search engines to allow Internet users to search for topics of interest by typing in a word or series of words relating to the topic. After receiving the request, the Internet search engine searches hidden invisible markers, called metatags, placed by website operators to identify the site's contents to the search engine. In principle, the metatag should accurately reflect the site's contents, thus enabling the search engine to match the viewer's interest with relevant sites.

In *Playboy*, plaintiff alleged that defendant had infringed plaintiff's rights by using plaintiff's trademarks as metatags to lure viewers interested in Playboy to defendant's site. Granting plaintiff's motion for preliminary injunction, the court concluded that defendant's use of plaintiff's mark as a domain name and as a metatag violated plaintiff's rights.

Trademark Misuse Not Permitted as Affirmative Claim

A federal district court in Illinois has rejected trademark misuse as an affirmative claim, limiting such misuse allegations to an affirmative defense only. *Juno Online Services, L.P. v. Juno Lighting, Inc.*, 1997 U.S. Dist. Lexis 15699 (N.D. Ill. 1997) Defendant, owner of a trademark registration for JUNO, claimed rights in plaintiff's domain name "juno.com." Plaintiff, an Internet service provider, filed a declaratory relief action, alleging that defendant had misused its trademark by attempting to put plaintiff out of business by requesting cancellation of plaintiff's domain name. The court rejected plaintiff's claim, finding no legal precedent for a trademark misuse claim and reasoning that no such basis existed because a trademark holder cannot prevent a competitor from selling a product (as is the case with patent misuse), only from using the holder's name in connection with the product.

Former Employees Prevented From Use Of Customer Lists They Helped Develop

In *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514 (1st Dist. 1997), Morlife, a roofing company, brought suit for trade secret misappropriation against its former employees who started their own roofing company. The trial court enjoined the defendants from soliciting customers based on their knowledge of Morlife customers and awarded damages resulting from unjust enrichment of customers already attained from improper solicitation of these customers. The trial court found that Morlife's customer list was a trade secret because the list was developed over a period of years and included economically valuable information such as pricing, particular roofs, and roofing needs of each customer. Moreover, the trial court found that Morlife made reasonable efforts to maintain the secrecy of its customers' identity by limiting circulation of the list and advising employees that the customer information was valuable and confidential. In affirming the trial court, the First Appellate District of the California Courts of Appeal reasoned that the customer list was not readily ascertainable, was reasonably protected, and had economic value because its disclosure would allow a competitor to direct its sales efforts to those customers who willingly use a unique service or product. Further, the appellate court reasoned that the defendants did misappropriate the customer list because they solicited business from customers they knew of from the customer list despite knowing that the customer list was considered confidential and economically valuable.

Ninth Circuit Adopts Copyright Misuse Defense Against Unrelated Infringements

In *Practice Management Information Corp. v. American Medical Association*, 121 F.3d 516 (9th Cir. 1997), the Ninth Circuit held that copyright misuse is a complete defense to copyright infringement even when the defendant was not a party to the overreaching contract. The American Medical Association ("AMA") owned the copyright in a work which included procedures that had been adopted by a federal agency as the standard for preparation of Medicare and Medicaid forms. Plaintiff sued for a declaration that the AMA's copyrights in the work were invalid. The Ninth Circuit held that a license between the AMA and the agency that was conditional on the agency's promise not to use a competitor's product constituted a misuse of the copyright by the AMA.

Right to Revise a Collective Work Includes Electronic Publication

In *Tasini v. New York Times Co.*, 972 F.Supp. 804 (S.D.N.Y. 1997), a New York federal court held that publishers are entitled to place contents of their periodicals into electronic databases and CD-ROMs without the permission of writers whose contributions were included in the periodicals. Plaintiffs, who were freelance writers, filed suit for copyright infringement against its publishers for republishing their works in electronic formats, arguing that the publishers were authorized to use their articles in print version only. The court found that the periodicals are "collective works" and that the publishers' copyright in the collective works coexists with the authors' copyrights in their articles. A collective work copyright is presumed under the Copyright Act to give its creator the privilege of reproducing and distributing each contribution as part of that collective work, any revision of that collective work, and any later collective work in the same series. Revisions of the collective work are permitted only when the new collective work preserves the selection or arrangement of the preexisting collective work. Although the electronic versions failed to reproduce the original arrangement from the print periodicals, the court found that the original selection element was preserved, thus making the electronic works permissible revisions.

Intellectual Property Bulletin Editorial Staff

Fall 1997

Editor
Stuart P. Meyer

Assistant Editors
David C. McIntyre
John T. McNelis

Article Contributors
Tim Alan Covington
Stuart P. Meyer

Update Contributors
William P. Fitzpatrick
Christine L. Hoang
Tina M. Lessani
Rajiv P. Patel