



FENWICK & WEST LLP



Intellectual Property Bulletin

Fenwick & West LLP — Winter 1999



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, 1999 Fenwick & West LLP. All Rights Reserved.



Intellectual Property Bulletin

Winter 1999

Table of Contents

U.S. Encryption Export Policy Update (Updated February 2000)

Online Service Providers: The New Copyright Enforcers 1

Quick Updates 4

 Theft of a Computer Disk Containing a Compilation of Publicly Available Information
 Is Not a Violation of Trade Secret Law 4

 Attorney-Client Privilege Applies to Email Messages (For Now) 4

 Federal Circuit Applies Supreme Court's Two-Part Test in Pfaff to
 Invalidate Patent 5

 Court Prevents the Use of Metatags That Could Misdirect a User
 Who Is Performing an Internet Search 5

 Mere Reference to a Company's Trademark on a Web Site Is Not Enough to Confer
 Personal Jurisdiction 5

 Copyright Term Extension Is in Dispute 6

 Second Circuit Holds That the Use of West Publishing's Pagination of Judicial
 Decisions Does Not Constitute Copyright Infringement 6

Editorial Staff 7

Online Service Providers: The New Copyright Enforcers

by Laurel Jamtgaard

Offering legal advice to online service providers (OSPs) entails stepping into a morass of evolving legal rules, government regulations, visionary predictions, industry standards and customer expectations. Title II of the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512, signed by President Clinton on October 28, 1998, has provided what will hopefully be some “dry land” for OSPs with regard to one serious issue—liability for copyright infringement.

In a matter of a few years, OSPs, from the behemoth America Online (AOL) to the local community college, have become fundamental players in the Internet arena. OSPs have gained this stature while walking a high wire of potential liability for copyright infringement taking place on and through their systems. As the gatekeepers for the public’s access to the Internet, OSPs have the ability to monitor subscriber activities and to remove or disable access to problematic files or Web pages. With the DMCA, Congress has begun to direct this power toward curtailing copyright infringement.

Title II of the DMCA, entitled “Online Copyright Infringement Liability Limitation,” offers OSPs several valuable defenses or “safe harbors” to copyright infringement claims, but in order to take advantage of most of them, OSPs will need to play a role in the enforcement of copyright law. For example, if a photographer provides notice to AOL that an infringing copy of one of his or her photographs is being stored on AOL’s system, perhaps decorating a subscriber’s personal home page, AOL will need to take steps to remove or disable access to the allegedly infringing image file.

The new law includes some procedural safeguards to enable the party whose file was removed to challenge the action. At some point, a given controversy can weave its way into court, but with this new law, it will be the service provider, not a judge, providing injunctive relief for copyright infringement on the front lines of cyberspace.

The definition of “online service provider” in Title II is quite broad and has different meanings for different safe harbors. For the safe harbor relating to transmission and transient storage it means “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” §512(k)(1)(A). For the other safe harbors, however, the term expands to include “a provider of online services or network access, or the operator of facilities therefor.” §512(k)(1)(B).

With this broad definition, any organization that stores or reproduces online content on behalf of other parties, even if it is just hosting an electronic mail service or providing a Web search tool, should take a close look at the carrot offered by the DMCA.

The Safe Harbors

Title II creates four “safe harbor” defenses for services typically offered by OSPs. Each of the activities can involve making unauthorized copies of copyrighted works and therefore in the absence of the “safe harbor” defenses could expose the OSP to direct, contributory or vicarious liability.

(1) Transmission and Transient Storage 17U.S.C. § 512(a) (1998)

This safe harbor offers protection for transmitting, routing or providing connections to material through an OSP’s system. In general, to invoke this defense the transmission of the allegedly infringing material must have been initiated by someone other than the OSP and must be carried out by way of an automatic technical process without selection of the material or its recipients by the OSP. Furthermore, the OSP must strictly limit maintenance of any copies of the material generated in the course of the transmission and may not alter the content of the material while it is being transmitted.

(2) System Caching of Copyrighted Materials 17U.S.C. § 512(b) (1998)

This safe harbor seeks to allow service providers some ability to “cache,” or temporarily store, popular materials in order to improve performance for end users and to reduce network traffic. At the same time it protects the ability of the originator of the material to set limits on the frequency or mode of caching.

This defense has several specific requirements. Among them, the OSP must transmit the material without modifying its content; comply with rules concerning refreshing, reloading or other updating of the cached material; and limit access to only those users who have met the conditions placed on the material by the originator *e.g.*, passwords or fees.

(3) System Storage of Copyrighted Materials on Behalf of Users 17U.S.C. § 512(c) (1998)

This safe harbor is perhaps the most important for OSPs. It limits OSP liability when the OSP’s users or subscribers store infringing materials on the OSP’s system. For this safe harbor, an OSP must have been unaware that the stored material was infringing and must not have been aware of facts or circumstances from which the infringing activity was apparent. Upon obtaining such awareness or direct knowledge, the OSP must act expeditiously to remove, or disable access to, the material or link following the procedures presented in the statute.

(4) Information Location Tools 17U.S.C. § 512(d) (1998)

This safe harbor highlights the statute’s broad definition of OSP. It limits the liability of an OSP for referring users to infringing materials at remote sites by way of search tools,

hypertext links, directories of site addresses or the like. An OSP must have been unaware that the “linked-to” material was infringing and must not have been aware of facts or circumstances from which the infringing activity was apparent. Upon obtaining such awareness or direct knowledge, the OSP must act expeditiously to remove, or disable access to, the material or link following the procedures presented in the statute.

Advising Online Service Providers

Several of the safe harbors require that an OSP designate an “Agent to Receive Notice of Claimed Infringement” with the Copyright Office. A closely related step is to publish the Agent’s contact information on the OSP’s Web site accessible by the general public.

OSPs also need to adopt, reasonably implement and inform users of a policy for the termination of access by users who are repeat copyright infringers, § 512(i)(1). The likeliest way to do this will be to add a clause to the OSP’s subscriber agreement or the site’s “Terms of Use.”

Perhaps the most difficult step will be to define reliable, internal procedures for responding to (a) notices of infringement and (b) “awareness” of infringement. The DMCA provides some guidance as to what constitutes an “effective” notice from a copyright holder, § 512(c)(3). But even in the absence of “actual notice” an OSP is obligated to act if it has awareness “of facts or circumstances from which infringing activity is apparent,” § 512 (c)(1).

OSPs are shielded from liability for claims based upon the OSPs “good faith disabling of access to, or removal of material” based upon actual notice or awareness “regardless of whether the material [. . .] is ultimately determined to be infringing,” § 512(g)(1). The Act also includes important guidance on how to handle “counter-notification” from the person whose material was removed, § 512(g)(3).

It is important to recognize that the safe harbors are supplemental to other defenses available to OSPs under copyright law, including the “fair use” doctrine. But as a practical matter, upon receiving notice from a copyright holder, OSPs may prefer to follow the procedures to remove the allegedly infringing materials rather than relying on a “fair use” defense.

Because of the numerous requirements imposed by the DMCA and the lack of case law to clarify the requirements, advising clients is difficult at this point. But many OSPs have already registered with the Copyright Office and are gradually meeting the notice requirements on their Web sites, so some guidance can be gained by looking at what others have done. The most important piece of practical advice for OSPs is to act expeditiously to comply with the statute because, for most, the safe harbors will be worth the effort.

The deal struck in Title II of the DMCA has been viewed as a “win-win” for the copyright holders and the online service providers. It reflects a compromise reached after a long and contentious negotiation process among the respective industry representatives. This move may increase the potential for OSPs to receive other, non-copyright-related, enforcement assignments in the future. Only time will reveal what impact the DMCA’s version of “privatized” copyright enforcement will have on other members of the Internet community and on the overall balance of rights between copyright holders and the general public. One thing is sure: Providing legal advice to online service providers will not get dull anytime soon.

Quick Updates

Theft of a Computer Disk Containing a Compilation of Publicly Available Information Is Not a Violation of Trade Secret Law

In *Capital Asset Research Corp. v. Finnegan*, 160 F.3d 683, (11th Cir. 1998), plaintiff Capital Asset Research Corp. (“CARC”) brought suit against defendants Finnegan and Breen Capital Holdings, Inc., (“Finnegan”) for misappropriation of trade secrets. The district court found that Finnegan, a former employee of CARC, misappropriated a computer disk that contained trade secrets under Georgia law. The alleged trade secrets included a compilation of property-specific information, a national database on tax redemption behavior and final bid guidelines for tax deeds sold at auction. The U.S. Court of Appeals for the 11th Circuit reversed. The court held that these items did not qualify as items that were protectable as trade secrets under Georgia law. The court reasoned that the items were not trade secrets because the property data and information were available from public sources. Therefore, an informed and experienced bidder could and would gather the data and information from those public sources. Further, the informed and experienced bidder would use the data and take the same steps described in the bid guidelines when making a purchasing decision.

Attorney-Client Privilege Applies to Email Messages (For Now)

In *Amylin Pharmaceuticals Inc. v. University of Minnesota*, 48 U.S.P.Q. 2d 1861 (S.D. Cal. 1998), the district court applied the attorney-client privilege to emails. Although the court questioned whether there can ever be an expectation of confidentiality in email messages such that those messages can be privileged, the court noted that problems with the confidentiality of email is an issue that the public has only become aware of in recent times. Accordingly, the court denied in part a motion to compel discovery of withheld documents, some of which were email messages, on grounds of the attorney-client and joint defense privileges.

Federal Circuit Applies Supreme Court's Two-Part Test in Pfaff to Invalidate Patent

In *Weatherchem Corp. v. J. L. Clark, Inc.*, 49 U.S.P.Q. 2d 1001 (Fed. Cir. 1998), the Court of Appeals for the Federal Circuit (CAFC) held that evidence of a signed purchase agreement and detailed drawings of an invention before the critical date established an offer for sale sufficient to invalidate the patent under the on-sale bar of §102(b). Applying the two-part test from the recent Supreme Court decision *Pfaff v. Wells Electronics, Inc.*, 48 U.S.P.Q. 2d 1641 (1998), the CAFC asserted that it was immaterial that the later patented product was not delivered and no money was exchanged until after the critical date. Rather, the CAFC concluded that the signed purchase agreement indicated that the product at issue was the subject of a commercial offer and acceptance before the critical date.

In applying the second part of the *Pfaff* test, the CAFC determined that the invention at issue was ready for patenting before the critical date. Specifically, the court found that the invention was "ready for patenting at the time of its depiction in the 2-8-85 drawing [which was before the critical date], even though [the inventors] continued to fine-tune features not claimed in the patent." The court reasoned that the detailed drawings at issue were sufficiently specific to enable a person skilled in the art to practice the invention.

Court Prevents the Use of Metatags That Could Misdirect a User Who Is Performing an Internet Search

In a recent decision further defining the rights to use Internet "metatags" (markers that are invisible to the public but are used to allow search engines to direct traffic to relevant Web sites), a federal court enjoined a defendant from using metatags to misdirect searches from a competitor's Web site. In *Niton Corp. v. Radiation Monitoring Devices, Inc.*, D. Mass. No. 98-11629-REK, November 18, 1998, the district court enjoined the defendant from using metatag descriptions on its Web site that are identical to those on the plaintiff's commercial Web site. The defendant had used as metatags terms relevant only to the plaintiff's site. The court concluded that as a result of defendant's actions, consumers using the metatag terms to conduct an Internet search would be referred to the defendant's site. Finding that consumers were likely to mistakenly believe that defendant was affiliated with plaintiff, the court granted preliminary injunctive relief.

Mere Reference to a Company's Trademark on a Web Site Is Not Enough to Confer Personal Jurisdiction

In *Conseco, Inc. v. Hickerson, Ind.* Ct. App. No. 29A04-9802-CV-85, November 14, 1998, an Indiana state appellate court concluded that the mere referential use of a company's trademark-protected name on a Web site is insufficient, absent other contact with the forum state, to confer personal jurisdiction. Plaintiff, an Indiana-based corporation, sued defendant, a non-Indiana resident, for trademark infringement and dilution, alleging that defendant's use of plaintiff's mark in the text of his Web site constituted infringement. The issue before the court was whether the defendant had sufficient contact with the state to

support personal jurisdiction. To determine whether defendant had purposefully availed himself of the state's protections, so as to create personal jurisdiction, the court borrowed the test created by the *Ninth Circuit in Cybersell, Inc. v. Cybersell Inc.*, 130 F.3d 414 (9th Cir. 1997). In *Cybersell*, the Ninth Circuit held that in determining whether there are sufficient contacts to warrant the exercise of personal jurisdiction in the context of a Web site, the court must look at the site's level of interactivity and the commercial nature of the information exchanged. Applying the test to the immediate facts, the court concluded that defendant's discussion of the plaintiff corporation on his Web site was insufficient to create personal jurisdiction.

Copyright Term Extension Is in Dispute

The Sonny Bono Copyright Term Extension Act of 1998, Pub. L. No. 105-298, 112 Stat. 2827 ("CTEA") was signed into law on October 27, 1998. The CTEA adds 20 years to the term of most copyrights, giving pre-1978 works a term of 95 years and post-1978 works a term of 70 years after the death of the author (or 95 years in the case of works made for hire).

On January 11, 1999, Eric Eldred and the Eldritch Press filed suit to overturn the CTEA. *Eldred v. Reno*, No. 1:99CV00065 (D. DC 1999). Eldred contends that the CTEA is an attempt by Congress to circumvent the constitutional requirement that copyrights be granted only for "limited" times to authors. In 1962 the maximum copyright term was extended to 59 years. Under the CTEA, the maximum copyright term in 1998 was extended to 95 years. Over a period of 36 years, the maximum copyright term was extended by 36 years. Eldred argues that this pattern of retroactive copyright term extensions is evidence that, although a copyright term is nominally limited at any given time, it is in fact not limited.

Second Circuit Holds That the Use of West Publishing's Pagination of Judicial Decisions Does Not Constitute Copyright Infringement

On November 3, 1998, the United States Court of Appeals for the Second Circuit upheld a district court decision holding that publishers of CD-ROM compilations of judicial decisions do not infringe the copyrights of West Publishing Corporation ("West") by including "star pagination" to indicate the location of page breaks in the West compilations. *Matthew Bender & Co. v. West Publishing Co.*, Docket No. 97-7430 (2d Cir. 1998). West had appealed from the district court's granting summary judgment to Matthew Bender & Company, Inc., and Hyperlaw, Inc., who sought a declaratory judgment of non-infringement. West argued that the use of star pagination by the defendant's publications allowed users to "perceive" Wests' arrangement of cases. Citing the Supreme Court in *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 111 S. Ct. 1282 (1991), the Second Circuit held that copyright protection in a factual compilation is particularly "thin," and that, although a user could utilize the star pagination in order to recreate West's arrangement of cases, the arrangement on the CD-ROMs is not substantially similar to West's arrangement. The court noted that, in so holding, it differs from the Eighth Circuit in *West Publishing Co. v. Mead Data Central, Inc.*, 799 F.2d 1219 (8th Cir. 1986).

Intellectual Property Bulletin Editorial Staff

Winter 1999

Editor

[Stuart P. Meyer](#)

Assistant Editor

[John T. McNelis](#)

Article Contributors

[Edward J. Radlo](#)

Laurel Jamtgaard

Update Contributors

M. Trinnie Arriola-Kern

Christine L. Hoang

[Rajiv P. Patel](#)

Steven D. Young