FENWICK & WEST LLP

Intellectual Property Bulletin

Fenwick & West LLP — Spring 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.

FENWICK & WEST LLP

Intellectual Property Bulletin

Spring 1999

Table of Contents

Private Information For Sale: The Coming Of Online Privacy Regulations

by Jeremy S. Woodburn

One of the most valuable intangible assets of many on-line businesses is the information that they are able to collect about the users of their services, and possible government regulation of the collection and use of that information could significantly change the value of that asset. The Internet has significantly enhanced the ability of businesses to collect, store, use and exchange information about individuals.

For example, information service providers and Web-site proprietors typically require users to provide home addresses, telephone numbers and other personal information in order to obtain services, and have the ability to collect email addresses, entered text, visited Web sites, specific Web pages and parts of pages on which a user clicks. Businesses that are more traditional vendors of products or services also collect information over the Internet, through registration and mailing list submissions, for example.

All of this information, which can be identified with a specific person, is generally referred to as "personally identifiable information" ("PII") and is valuable to advertisers and direct marketers, among others, who can use this information to more accurately target advertising to consumers. The tension between the value and increasing availability of this information and mounting public and legislative concern has led to several national and international efforts to promote regulation of the uses of PII.

Online businesses must understand, anticipate and prepare for the type of regulatory regime that will likely be imposed. This need is underscored by two recent actions of the Federal Trade Commission (FTC). In June 1998, the FTC delivered a report to Congress in which it made recommendations for future privacy regulation. Federal Trade Commission, *Privacy Online: A Report to Congress* (June, 1998). The FTC report divided its recommendations into the following five categories:

Notice/Awareness: An entity should give notice of its information practices to each consumer before the entity collects any PII from the consumer. Notice should include the identity of all entities collecting, storing and receiving the information, the nature of the information collected, the uses of the information of all receiving entities, the procedures used to maintain the security of the information and the consequences of refusal to provide the information.

Choice/Consent: Entities collecting and using PII should allow consumers to consent to all uses of the information. The consumer's opportunity to consent should be clear, easily available and as detailed as is reasonable under the circumstances.

Access/Participation: Each consumer should have an effective right to access his or her PII and to correct errors or gaps in the information.

Integrity/Security: Collecting entities should take steps to ensure that PII in their control is neither corrupted nor accessed inappropriately.

Enforcement/Redress: The FTC opined that effective enforcement mechanisms for privacy regulations should be implemented, although the FTC did not offer concrete recommendations.

The report also emphasized the limited role of the FTC in such enforcement. However, it took the FTC less than two months to find and resolve a situation in which it had jurisdiction. On August 13, 1998, the FTC announced that it had reached agreement with Geocities Corporation on a consent order regarding Geocities' collection, use and disclosure of PII of users of Geocities' service. Geocities is an Internet service provider that offers its subscribers various services, including Web-page hosting and email. The FTC issued a complaint against Geocities alleging that Geocities had misrepresented to its subscribers its practices with respect to the collection, storage, use and disclosure of subscriber PII. Although the complaint, and subsequent consent order, also focused on the use of information collected from children, the discussion here focuses on the more general concerns of the FTC and the FTC's responses.

According to the complaint, Geocities had made representations to its subscribers that it would not share any of their PII with third parties without their permission. The FTC alleged that Geocities instead regularly provided subscriber PII to third parties without the consent of the subscribers. The FTC alleged that these misrepresentations constituted deceptive acts and practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45 (1994).

Geocities agreed to submit to a consent order controlling its privacy policies, which the FTC entered on February 5, 1999. Decision and Order, In the Matter of Geocities, Docket No. C-3850, File No. 982 3051. Under the consent order, Geocities is required to: (1) provide notice to all users of the service of Geocities' practices with respect to PII, including the nature of the information collected, the use to which Geocities will put the information, third parties to whom Geocities will disclose the information, and the procedures for access to and deletion of PII; and (2) allow users of its service to have access to the PII relating to them, and to instruct Geocities both to remove their information from Geocities' databases and the databases of third parties, and not to disclose any of their information to any third party.

Authorities other than the FTC have also begun to address online privacy, and the trends are similar to those in the FTC's actions. For example, the European Union Parliament and

Council issued Council Directive 95/46 of 24 October 1995, 1995 O.J. (L 281) 31, which sets forth principles on which its European Union member countries are to base laws regarding the privacy of individual data. Under the Directive, the requirements for notice, consent, access, integrity and security are similar to the principles stated in the FTC report to Congress and implemented in the Geocities consent order.

The Consumer Internet Privacy Protection Act of 1999, H.R. 313, 106th Cong. 1st Sess. (1999), is a bill recently introduced in the United States Congress that would directly regulate the disclosure of PII collected through the Internet. H.R. 313, if enacted in its current form, would be less sweeping than the regulations proposed by either the FTC report or the EU Directive, but would require that every entity collecting PII through the Internet must, upon request, disclose to each individual the identity of recipients of any information of that individual, and would have to provide to each individual access to all information that the entity collects regarding the individual. The individual would have the opportunity to correct any error in such information. Moreover, under H.R. 313, an online business would not be permitted to disclose any PII of an individual to a third party without the subscriber's prior freely-signed informed written consent to the disclosures to be made.

Despite the current lack of enacted legislation, online businesses should assume that they will at some point in the near future be subject to regulations consistent with the FTC report and EU Directive (and various state and international laws). Online businesses should take certain steps now to prepare for that future regulation of their use of PII. These steps include: (1) implementing a notice and consent procedure, by which subscribers are provided with clear notice of the online business's uses of their PII, are then allowed to consent to or opt out of such uses, and which includes an option for subscribers to revoke such consent; and (2) developing a technical framework able to inform subscribers of all the PII the business collects about them, where and how that information is stored and to whom it is disclosed. This technical framework should also allow subscribers to correct inaccurate information and prevent further disclosure of their information.

To protect their information assets, online businesses should also divide their collection of subscriber PII into administratively separate databases, segregated according to whether or not the relevant subscribers have consented to the use and disclosure of their information in writing, online or have not consented. This allows online businesses to quickly respond to most of the regulations likely to be enacted regarding consent by individuals.

Moreover, online businesses should avoid obligating themselves to provide PII of subscribers to third parties, or at least make such obligations contingent on future regulation, so that they are not caught between regulatory requirements and contractual obligations.

Avoiding International Trademark Disputes On The Internet

by Karen M. Kitterman (kkitterman@fenwick.com)

"When all of your products are scattered about the Web and can be compared in a flash to all of your competitor's products, there's one thing that becomes more important than all of the technology put together: your brand." (Jim Sterne, *World Wide Web Marketing*, second edition, page 370). Trademarks communicate with tremendous efficiency. We turn reflexively to trademarks, to brands, in the Internet's information barrage. Trademark rights are territorial, however, and the Internet is global. Consequently, many international disputes are arising from the use of trademarks on the Internet.

The global nature of the Internet suggests that regional, possibly global, trademark policy agreements may one day exist. Business can reduce the risk of international trademark problems by taking precautionary actions before using their trademarks on the Internet. Such actions include conducting international trademark searches, registering trademarks abroad, researching marks for cultural clearance and employing registrations on national top-level domains. These precautions are trademark-specific, however, and numerous other laws may apply to Web-site business uses, *e.g.*, international prohibitions on comparative advertising, restrictions on advertising to children, decency laws and export restrictions.

The Internet has made determining a trademark's availability more difficult. Before the advent of the Internet, one could clear a trademark with a certain level of confidence by searching the jurisdiction in which the mark would be used. If no party had prior rights, a business could begin using its mark without significant fear of demand letters or injunctions. Now, when almost all businesses have a presence on the Internet and thus have their marks present in every corner of the world, clearance is fraught with uncertainty. Searching every jurisdictions' trademark registries and common law trademark uses is ideal, but also beyond the budget of virtually all businesses, especially when a mark is intended for the U.S. market only (albeit through an internationally accessible Web-site).

International trademark searches can be conducted online (for a limited number of countries), through U.S. search companies or through international counsel. Those conducted by international counsel are typically the most thorough, but are also the most expensive. For searching, a business should determine where it intends to market the product or service on which its trademark will be used. Future target markets also should be considered. Thus, if a company intends to market in the United States in the summer and in Japan the following year, seeking trademark clearance in both countries now may prevent that company from having to adopt a "plan B" mark in the future, if the first choice trademark is registered already in Japan. While clearance in target markets reduces risks, it cannot eliminate all risks because when orders can be received via the Internet, no one can

know beforehand the countries in which all customers are located. A business, for example, may anticipate local orders only, and then receive multiple orders from Portuguese customers, in whose country the mark may not be available for use.

In the United States, trademark rights are acquired through use and enhanced through registration. Most countries, however, grant trademark rights to the first party to register a mark. Consequently, registering a mark in key international markets is necessary to prevent others from registering it first, which could block a company's right to the use of its own mark on a Web site aimed at that country's customers.

When considering a trademark for Internet use, a company should consider also how a trademark will be received in other countries. This may prevent a business from adopting disastrous symbols of goodwill. Appreciating cultural differences, for example, can mean the difference between a product's regional failure or success.

Logos too may carry different meanings abroad. Hand gestures, for example, are interpreted in vastly different ways around the world. The American "okay" signal translates to "money" in Japan, "worthless" in southern France and an offensive gesture in Brazil and Germany. Thus, a Web-site logo showing our "okay" hand sign may alienate entire regions, while simultaneously misinforming others.

Sometimes cultural and legal trademark issues blend together. Americans, for example, would likely perceive a Web site's interactive Winnie-the-Pooh trademark as savvy advertising. In Denmark, however, the Consumer Ombudsman warned Walt Disney that its Web site's interactive games, quizzes and prize competitions violate both the Danish rules of good marketing practice and the International Chamber of Commerce's codex on good marketing practices, which prohibit taking advantage of children's natural credulity or lack of experience. ("Interactive Marketing to Children and Young Persons," the [Danish] National Consumer Agency, February 24, 1997).

While the Danish Ombudsman noted that "[t]he Internet is a global media which means that Disney's commercials are not only aimed at the American market but at many others also—including the Danish market." (*Id.*), Disney responded by claiming that its marketing complies with American law and that it is not obliged to comply with Denmark's laws. The Ombudsman has pledged to monitor the situation closely and did not rule out future action against Disney, whose site now states that those who choose to access it from abroad are responsible for compliance with local laws.

Thus, while a Web site's trademark use may violate foreign laws, a foreign court may not necessarily assume jurisdiction over a U.S. company for those violations. U.S. companies with direct dealings, assets or subsidiaries in foreign countries can be less sure, however,

that they are not subject to such jurisdiction. Within Europe, for example, the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters can bring unexpected jurisdictional results.

The Brussels Convention governs jurisdiction and enforcement of judgments in signatory countries (principally European Union countries) and gives plaintiffs the option of suing where a harmful event occurred. Thus, in *Mecklermedia Corporation v. D.C. Congress GmbH*, CH 1996\m\7266 (High Court of Justice, Chancery Division, March 7, 1997), an English court found jurisdiction over the owner of a Web site based in Germany, when a plaintiff showed that the German site's trademark use caused harm and damages within England.

The German defendant argued that its trademark use was legal because it owned a German registration for the mark and was suing the plaintiff's licensees in Germany for infringement of that registration as well. The English court was not persuaded. It found jurisdiction and refused also to allow consolidation of the two actions in Germany. Companies with subsidiaries domiciled abroad should thus be cautioned that national borders may not shield them in Internet trademark actions.

England is not the only European country finding trademark violations through foreign-based Web sites. French courts, for example, consider themselves the proper forum to hear all trademark cases arising out of Web sites accessible within France.

Fortunately, while careless use of Internet domain names may create disputes, domain names also can be used to prevent disputes. Thus, utilizing national domain names is a good strategy to prevent international trademark problems. Each country has its own top-level domain. (For example, domain names ending in .dk are registered in Denmark.) Clients can address consumers in a specific country through a Web site using that country's top-level domain. Content on a country-specific Web site can then be tailored to comply with that country's trademark laws, as well as other territory-specific regulations (*e.g.*, comparative advertising restrictions).

Numerous multinational companies now register their key trademarks as domain names in countries where they have subsidiaries. Thus, many businesses now treat domain name registration on a jurisdictional basis, much as they do registration of other intellectual property rights. This approach can demonstrate a company's good faith in trying to comply with territorial laws, but it is costly and cannot eliminate the fact that Web sites remain accessible from any territory, regardless of top-level domain.

Thus, no one can predict how foreign courts will rule on every Internet trademark use. A company's chance of avoiding disputes improves dramatically if it searches, clears, and registers marks in international target markets, utilizes national top-level domains and consults with knowledgeable U.S. and international counsel.

Quick Updates

Telephone Companies are not "Owners" of Digital Loop Carrier Software Under §117 of The Copyright Act

The U.S. Court of Appeals for the Federal Circuit held in *DSC Communications Corp. v. Pulse Communications, Inc.*, 50 U.S.P.Q.2d (BNA) 1001 (Fed. Cir. 1999) that telephone companies were not "owners" of digital loop carrier software created by DSC Communications Corp. ("DSC") and were therefore not protected by §117 of the Copyright Act, which allows a "lawful owner" of a copy of software to create additional copies in order to use the software.

Defendant Pulse Communications ("Pulse") manufactured telecommunications equipment to replace equipment manufactured by DSC. The equipment, upon power-up, would automatically create a temporary copy of DSC's software stored in other equipment. DSC sued Pulse for contributory copyright infringement, as Pulse's customers were making unauthorized copies of DSC's software each time they used Pulse's equipment. The Federal Circuit reversed a lower court ruling for Pulse, finding that the telephone companies were not "owners" of any copies of the software. In the language of its license agreements, DSC had retained ownership of the copies of software used by the telephone companies, granting them only the right to use the software with DSC's equipment.

Registered Computer Program Found Infringed by Copying of an Unregistered Later Version

In *Montgomery v. Noga et al.*, 49 U.S.P.Q.2d (BNA) 1961 (11th Cir. 1999), the Eleventh Circuit U.S. Court of Appeals ruled that an unregistered version of a computer program could be considered a derivative work of an earlier, registered version. Robert Montgomery, the plaintiff, created several versions of the VPIC image viewer program, but only registered one of these versions, VPIC 2.9a. The defendant, Rebecca Noga, included a later version of the VPIC program, version 4.3, on CD-ROMs she sold. The trial court found that Noga had committed copyright infringement, and awarded Montgomery attorney's fees and costs in addition to infringement damages. Noga appealed, contending that the version of the program she had copied had not been registered.

The appeals court upheld the lower court ruling, holding that the inclusion of 70% of the source code of the registered version in the unregistered version made the unregistered version a derivative work. The court found that by copying the unregistered version, which relied on source code from the registered version in order to operate, the defendant had infringed the registered copyright in the registered version.

Fourth Circuit Decision Narrows Federal Dilution Claims by Requiring Eevidence of Actual Dilution

The Fourth Circuit recently narrowed the scope of federal law prohibiting trademark dilution, holding that a federal dilution claim requires actual consummated dilution, not merely the "likelihood of dilution." *Ringling Bros-Barnum & Bailey Combined Shows Inc. v. Utah Division of Travel Development*, 1999 U.S. App. LEXIS 4179 (4th Cir. 1999). The plaintiff, owner of the mark THE GREATEST SHOW ON EARTH, brought suit against defendant for its use of the slogan THE GREATEST SNOW ON EARTH in connection with its travel and tourism business, alleging that defendant had diluted plaintiff's mark by blurring the mark's identity. Plaintiff argued that dilution required only such similarity as to create in viewers an "instinctively mental association" of the two marks. The Fourth Circuit rejected plaintiff's argument, instead concluding that the recently enacted federal statute was intended to prevent the loss of a mark's selling power and economic value, not the loss of the mark's uniqueness. For this reason, the court held that to prevail on a federal dilution claim, a plaintiff must show that the famous mark suffered actual harm to its economic value, defined as a lessening of its former selling power for goods or services. The court conceded that its interpretation would grant the federal dilution claim a narrower scope than that afforded by state claims.

Altering a Trademark Logo for a Consumer Criticism Web Site and Placing It in Close Proximity to Pornographic Sites Found not to Infringe or Dilute Plaintiff's Mark

In *Bally Total Fitness Holding Corp v. Faber*, 29 F. Supp.2d 1161 (C.D. Cal. 1998), a federal district court upheld defendant's use of plaintiff's marks on defendant's "gripe site" aimed at disseminating consumer criticism against plaintiff. Defendant operated a Web site which depicted plaintiff's stylized logo intersected by the word "sucks." In addition, defendant also operated several sites displaying nude images; all of defendant's sites could be found under the same domain name. Plaintiff brought suit alleging trademark infringement and dilution. The court granted summary judgment for the defendant. Deciding the infringement claim, the court ruled that, as a matter of law, defendant did not infringe plaintiff's mark because the parties' goods were unrelated. Turning to the dilution claim, the court held that because defendant's use was not commercial, defendant's use of plaintiff's logo did not violate plaintiff's rights. The court further found that even if defendant's use was commercial, defendant did not tarnish plaintiff's mark merely by operating its "pornographic" sites in close proximity to the "Bally Sucks" site or by creating links between all of the sites.

Video Demonstration of Invention to Conference Committee Chairman is not a "Public Use" under §102(b) Even Though There was no Express Confidentiality Agreement

In *Xerox Corp. v. 3COM Corp.*, 49 U.S.P.Q.2d 1772 (W.D.N.Y. 1998), the district court held that a single disclosure of a videotape demonstrating the invention of a patent to the co-chair of an industry committee conference did not constitute a "public use" under 35 U.S.C. § 102(b) even though there was no express confidentiality agreement between the inventor and the

committee co-chairman. The court provided several reasons for its holding. First, citing *Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261 (Fed. Cir. 1986), the court explained that the "presence or absence of [an express confidentiality agreement] is not determinative of the public use issue." Therefore, although there was no express confidentiality agreement between the inventor and the review committee, the reviewer had a professional ethical obligation to treat the videotape as confidential. Second, the demonstration of the videotape was not to "commercially exploit" the invention, but rather to obtain acceptance for a future scientific conference. Finally, with respect to public policy considerations, the court concluded that this was not a case in which an invention had been removed from the public domain after the general public had come to believe that the invention was freely available. Rather, during the critical period, the general public had no access to the video of the invention.

Economic Espionage Act of 1996 Found not Unconstitutionally Vague as Applied to Attempt and Conspiracy to Steal Trade Secrets

In *U.S. v. Hsu*, 1999 U.S. Dist. LEXIS 2626 (March 11, 1999), the U.S. District Court for the Eastern District of Pennsylvania ruled that the Economic Espionage Act of 1996 ("EEA") is not unconstitutionally vague as applied to the conduct of a defendant "charged with only the inchoate offenses of attempt and conspiracy (rather than completed offenses)" to steal trade secrets. In this case, defendants Hsu and two other accomplices (together "Hsu") were caught and charged with conspiring and attempting to steal pharmaceutical trade secrets from FBI agents posing as corrupt company employees. The defendants raised the defense that the statute was unconstitutionally vague because of the term "related to or included in a product that is produced for or placed in interstate or foreign commerce." The court disagreed, stating that the term was "readily understandable to one of ordinary intelligence" and that the defendants were well-versed in the technology involving the trade secrets. The defendants also raised the defense that the statute was vague because it did not define "reasonable measures" to keep the information secret, or what was meant by not "generally known" or "readily ascertainable" to the public. The court disagreed that the term "reasonable measures" was unconstitutionally vague. The court noted that the definition of trade secrets, in which the term is found, is widely adopted in 40 states. Further, California's criminal trade secrets statute was not found to be unconstitutionally vague despite having the term "measures." Moreover, in this case the defendants knew that the company took many steps to ensure that the technology at issue remained secret. The court was more troubled with the terms "generally known" and "readily ascertainable," which it referred to as "vaporous terms." Nevertheless, the court found that the terms as applied in this case were not unconstitutionally vague because there were numerous emails, telephone calls and discussions with the undercover FBI agents that indicated that the defendants believed the trade secret technology was not "generally known" or "readily ascertainable" to the public.

Intellectual Property Bulletin Editorial Staff

Spring 1999

Editor
Stuart P. Meyer

Assistant Editors
Diane L. Kort
John T. Mcnelis

Article Contributors
Jeremy S. Woodburn
Karen M. Kitterman

Update Contributors
M. Trinnie Arriola-Kern
Christine L. Hoang
Rajiv P. Patel
Steven D. Young