Texas Wesleyan Law Review

Volume 8 | Issue 3 Article 11

7-1-2002

Current On-Line Issues

Wei Wei Jeang Esq.

Robin A. Brooks Esq.

CURRENT ON-LINE ISSUES

Wei Wei Jeang, Esq.†
Robin A. Brooks, Esq.‡

I. INTRODUCTION

With the frenetic pace of technological development in the area of global communications, it is no wonder that consumers and businesses are adopting and taking advantage of these technologies before they are fully mature. The law is being refined every day. Most recently, the Supreme Court granted certiorari to decide whether Congress's recent twenty-year extension of the term of copyright protection is constitutional.[1] Hotly disputed topics include digital copyright and liability for trademark infringement from technologically-driven issues such as hyperlinking and metatag use.

A scenario with one of our clients illustrates some of the issues that are intertwined with building an Internet presence. Our client, ABC, Inc. (ABC),[2] is in the business of providing services to building managers and utility companies. Specifically, ABC prepares and sends

† Shareholder, Munsch Hardt Kopf & Harr, P.C., 1445 Ross Avenue, Suite 4000, Dallas, Texas; J.D., Dedman School of Law, Southern Methodist University, Dallas, Texas; B.S. Computer Engineering, University of Illinois at Urbana-Champaign; registered to practice patent law before the United States Patent and Trademark Office. wjeang@munsch.com.

‡ Associate, Munsch Hardt Kopf & Harr, P.C., 1445 Ross Avenue, Suite 4000, Dallas, Texas; J.D., The University of Texas School of Law, Austin, Texas; B.S. Electrical Engineering, Rice University; M.S. Electrical Engineering, The University of Texas; Co-chair, Privacy and Security Subcommittee for the State Bar of Texas; registered to practice patent law before the United States Patent and Trademark Office. rbrooks@munsch.com.

1. Eldred v. Reno, 239 F.3d 372 (D.C. Cir. 2001) (deciding that the Sonny Bono Copyright Term Extension Act, which added twenty years to copyright term of protection, is constitutional), *cert. granted*, 122 S. Ct. 1062 (2002) (mem.).

2. This pseudonym will be used in lieu of our client's name.

DOI: https://doi.org/10.37419/TWLR.V8.I3.10

bills to the building tenants for utility usage. Our client approaches us for legal counsel regarding providing these and other services online using the Internet.

Our client has no direct relationship with the building tenants, but does have a relationship with the utility service provider in performing billing functions for them. However, ABC does not collect or enforce these amounts due. Each tenant executes an agreement with his or her building manager. The agreement governs the tenant's receipt of utility services and provides that the tenant will receive utilities from a utility service provider and that he/she will be billed for these services by a third party billing entity (in many cases, although not specifically named, ABC). These tenants may receive utility service on an all-bills-paid status, where utilities for the building are apportioned between tenants using a selected algorithm. Alternatively, these tenants may be billed for their actual utility usage. In many cases, our client has the ability to receive utility data from a utility meter indicating the usage of that building or of that tenant.

This relationship has been successful in the brick-and-mortar world. Our client wanted to expand its service to the Internet to allow not only the tenants, but also the building managers, to access data online and to pay bills online. This business paradigm would allow our client to reduce costs, but also to generate revenue from alternative sources that would otherwise not be possible. The scenario presented a very controlled environment, where ABC would allow a user to login and view forms related to its account. For example, a tenant could login and view utility and payment information related to his account, whereas a building manager might login and review accounts related to her buildings, and each tenant's utility usage.

This move to the Internet, to our client's surprise, presented a variety of legal issues that must be dealt with. For example, who owns the data pertinent to these tenants? How does our client keep its server data secure? Who owns the copyrights and trademarks that will be used during the on-line sessions? After our client's initial foray into the U.S. market, what international issues arise when our client begins to service customers in the European Union or other countries? A closer inspection reveals that, with planning, our clients may embrace this move, because any "lurking dangers" may be avoided.

II. Ownership and Protection of Web Content/Data

A. *What Law Governs?*

Web content includes visible data such as trademarks, graphics, photographs, text (such as utility usage data or other aggregated data), domain names, and the arrangement of the visible material (*e.g.*, frames). Web content can also include invisible data such as HTML or applet code and metatags. This invisible data may be used

https://scholarship.law.tamu.edu/txwes-lr/vol8/iss3/11
DOI: 10.37419/TWLR.V8.I3.10

in, for example, search engine functions and deep-linking. Ownership to web content displayed may also be as an interest in functions provided by software or as a business method. So, who owns the data used and published on ABC's web site?

First, patent law in many cases may govern business methods or functions delivered by applet code; whereas trademark law usually governs the display and distribution of trademarks, service marks, domain names, slogans, and use of these terms in invisible code such as metatags. Copyright law may be applied to displays and distribution of graphics, photographs, texts, HTML code, applet code, forms, reports, and data such as utility usage or other aggregate data. In many cases, contract law may be used to alter ownership rights for these various intellectual property interests. In addition, data such as utility usage or other aggregated data may also be subject to ownership interests especially if it is a trade secret, or is considered personally identifiable information. Moreover, access to data residing on one party's server may be governed by the law of trespass to chattels. Lastly, the actions of deep-linking and framing may also be governed by unfair competition law.

Generally, online transactions involve a number of intellectual property issues that may be analogized to the brick-and-mortar world. For example, some online forms that may belong to our client or the utility companies most likely would enjoy the same copyright protection as they would offline. Similarly, trademark rights may be asserted against others for misappropriation, or deceptive or false representations of logos, slogans, or other marks. Other issues may not be as apparent to online users. The issues of metatags, deep-linking, and framing, to name but a few, arise with the dynamic nature of creating and using a website, and its interactive features.

As one example, consider the forms. First, these forms may enjoy some copyright and/or trademark protection. They are copyrightable to the extent they are not functional and otherwise fit the statutory framework. So, absent any agreements between the parties, each intellectual property interest belongs to its owner. Thus, depending on whose forms are displayed on the Internet, the owner could be the building owner, the utility company, or ABC, or all three could own an interest in the forms.

B. *Copyright*

One online issue arises with every website that collects information from its users. Many websites require interaction with their users and are thus data-driven. In our scenario, ABC would like to collect and aggregate the data that it receives from its users. It could then compile this data into a database, and organize this information in a variety of reports. For example, ABC could report tenant payment histories and other information to building managers regarding their

tenants. ABC might even be able to leverage this information as an asset—it could then sell the information to an interested third party, such as a credit card issuer. But who owns this data? Much of this data has been collected from the utility company or the building manager. As one example, the building managers typically collect information from tenants in their lease applications. At the time these tenants filled out these applications, they likely were not informed that such information might be published on the Internet. Even more importantly, they likely did not realize that this information would be sold or otherwise disseminated to third parties, nor that it would be integrated into a database with the utilities' information. Moreover, the tenants probably do not wish for their data to be used in this manner.

Databases are data collections that allow selection and arrangement of data by attributes that are set up in the database. As to database law, the U.S. has not stepped in to protect "sweat of the brow" efforts used to compile databases jettisoned by the U.S. Supreme Court in *Feist Publications, Inc. v. Rural Telephone Service Co.*[3] In that decision, the Court held that, to be protectible, the database must have some creativity or originality.[4] Although the U.S. Legislature has considered conflicting bills for the last four years, no law has emerged from Congress since the decision. Foreign jurisdictions, however, have typically differed from the U.S. in their approach to protecting legal ownership rights of data within databases. One example includes the European Union's (the EU) approach to ownership of non-copyrightable web content. The EU has established *sui generis* protection for otherwise non-copyrightable web content such as databases. The EU Directive on Database Protection[5] (the Database Directive) fills the gaps created by the U.S. Supreme Court's decision in *Feist*, which explicitly held that "sweat of the brow" investments by the data owners did not, by itself, create copyright protection in that data. The Database Directive provides for protection for a database owner's substantial investment as a required element, and does not require creativity or originality as does *Feist*. The Database Directive provides for a fifteen-year term, which is renewable if there has been substantial reinvestment in the database.[6]

These jurisdictional differences introduce some tension for those website owners who intend to conduct business with jurisdictions abroad. For example, any online transactions involving databases owned by an EU citizen must be concerned with the copyrightability

3. 499 U.S. 340 (1991).

4. *Id.* at 361.

5. Council Directive 96/9 1996 O.J. (L 77) 20, *available at* http://europa.eu.int/ISPO/ecommerce/legal/documents/396L0009/396L0009_EN.doc (on file with the Texas Wesleyan Law Review).

6. *Id.* at Article 10.

of that content. In the scenario with our client, as one example, were our client to host its data in the EU, our client's database content would most likely be protected under EU law. Thus, the U.S. utilities would likely not have any claim to such content and, moreover, may be subject to copyright liability in the EU should they misuse, misappropriate, or otherwise violate the Database Directive or other EU law.

In addition to copyright protection, clients should be advised as to special restrictions on personal data collected, distributed, and sold.[7] Thus, databases that include consumer data may also be subject to consumer privacy regulation in many jurisdictions. U.S. law regarding consumer data has converged to what the Federal Trade Commission calls "fair information practices."[8] However, the U.S.'s "opt-out" paradigm is considered too lax in other jurisdictions such as the EU, which follows an "opt-in" paradigm. Jurisdictions such as the EU prefer more stringent controls that protect consumers from *not* automatically consenting to their data being used unless they affirmatively opt-in to such uses, unlike the U.S. Because our client intends to move into an EU market, its goals in selling consumer data, such as those regarding payment histories, will likely be much more restricted than they are here in the U.S. But our client might elect to keep its EU operations entirely isolated from its U.S. operations. Circumstances may be even more complex for other types of clients. For example, a retail client operating a website that may *sell* goods to users in a multitude of jurisdictions, such as a www.gap.com, likely should concern itself about transnational data flows.

C. *Trespass-Database Content*

More recently, courts considered the legality of using automated processes such as a bot to access another's online database. In *eBay, Inc. v. Bidder's Edge, Inc.*,[9] the court found impermissible trespass to chattels because the defendant's unauthorized access interfered with the plaintiff's possessory interest in its computer system, thereby causing damage. The parties settled the case while the opinion was pending before the Ninth Circuit. The *Ticketmaster* court,[10] on the other hand, found insufficient evidence of harm to the chattel or obstruction of its basic function, and therefore, repeated access of the database

7. A more thorough discussion of privacy issues is beyond the scope of this Article.

8. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/toc.htm. These fair information practices include disclosure of information collected and how it will be used, to whom the information will be disseminated, how the consumer can correct information, and how the consumer can "opt-in" or "opt-out."

9. 100 F. Supp. 2d 1058 (N.D. Cal. Mar. 27, 2000).

10. *See* Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553, 54 USPQ2d 1344 (N.D. Cal. Mar. 27, 2000).

content was permissible. The *Ticketmaster* court appears to have been heavily influenced by particular facts in its case. For example, the *Ticketmaster* defendant actually directed more traffic to the plaintiff's website, and the nature of the data was factual and uncopyrightable.[11]

ABC was fortunately able to control the types of copyrighted material that would be used on its website. For example, both the utility company and ABC each has copyright interests in the forms, and any look and feel of the website that might be copyrightable. As with any business relationship, these copyright interests may be used subject to a contractual arrangement (*e.g.*, a license or other agreement).

D. *Trademark*

As to web content, the most typical trademark issues that arise include metatags and downloading and/or displaying company logos or other marks, whether or not framed.[12] Generally, online liability is similar to the brick-and-mortar scenario. Infringement may lie under either state or federal law for using another's mark in commerce so that it deceives a consumer into believing that the mark was sponsored or associated with his own. Thus, downloading and displaying logos or other images may be considered infringing if such deceptions occur. As discussed previously, online issues arise with metatag use, deep-linking, and framing.

Unfortunately, our client's brick-and-mortar business did not lend itself to consideration of any of these interests and thus, no agreements existed. In order to tighten up the legal arrangement between the parties, we recommended that our client enter into a contractual relationship with the utility companies that addressed these interests and allowed our client, at the very least, a royalty-free license to use, display, and transmit any of the utility company's copyrighted forms, trademarks or logos, or other interests.

Generally, however, websites may be liable for much more in the area of copyright or trademark infringement. Any content that includes text, music, artwork, images, software, graphics, sounds, or other data covered by U.S. copyright or trademark law must be considered. There are three other areas to also consider: a) framing; b) metatag usage; and c) deep-linking.

E. *Cases*

Recently, the Ninth Circuit decided framing and linking issues in *Kelly v. Arriba Soft Corp.*[13] The court held that "thumbnail" image

11. *See id.* at *4–6, 54 USPQ2d at 1345–46.

12. Although as most attorneys know, small differences in website addresses make a world of difference, domain names and liability in remedies for infringement of these domain names is beyond the scope of this Article.

13. 280 F.3d 934 (9th Cir. 2002).

use for identifying the Uniform Resource Locater (URL) locations of those original image locations in a search engine result is fair use. In *Kelly*, the defendant reproduced plaintiff's images as thumbnails in its search engine.[14] Thumbnail images are smaller, low-resolution images (in some cases about the size of a U.S. postage stamp) that may be transferred very quickly from one site to another, but give the viewer an idea of the content of the image. These are typically utilized for indexing purposes, and a search engine must copy the thumbnail image to allow users to recognize the content and decide and whether to pursue more information about the image and/or its original website. Plaintiff sold and licensed his full-sized images on his own website to his own customers.

In *Kelly*, the court found that the defendant's use of the thumbnail images for information-gathering or indexing purposes caused no harm to the plaintiff's ability to license his images, nor was there any impact on plaintiff's market.[15] The defendant, however, also linked to and framed plaintiff's full-sized images after a user would click on the thumbnail images returned by the search engine. This required image importation directly from plaintiff's site while framing those images within defendant's own website. The court found that this was not fair use.[16] While Judge Nelson noted that Arriba's use of the images was for a commercial purpose, he reasoned that this use was more incidental than exploitative (that is, Arriba was not selling Kelly's images or using them directly to promote its website; rather, the images were among thousands of others in Arriba's database).[17] In balancing the factors, the court found that this was not a purpose different from plaintiff's; that image placement in a frame is not transformative use; that such full-sized display infringed plaintiff's exclusive right to display, transmit, and publish his original images (*i.e.*, his exclusive right to display publicly).[18]

Metatag use has been sharply criticized as seen in a number of cases involving *Playboy Enterprises, Inc. v. Calvin Designer Label*,[19] *Playboy Enterprises, Inc. v. Asia Focus Int'l, Inc.*,[20] and *Playboy Enterprises Int'l, Inc. v. Global Site Designs, Inc.*[21] Metatags are textual keys that are used in software code to be found by search engines, and are typically not viewed by a user surfing online. In most cases, courts have found unlawful such use by competitors of a mark because the defendants typically: "purposefully employed deceptive tactics to at-

14. *Id.* at 938.
15. *Id.* at 944.
16. *Id.* at 940–44.
17. *Id.* at 940. *See also* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1015 (9th Cir. 2001).
18. *Kelly*, 280 F.3d at 947–48.
19. 985 F. Supp. 1220 (N.D. Cal. 1997).
20. No. Civ.A. 97-734-A, 1998 WL 724000 (E.D. Va. Apr. 10, 1998).
21. No. 99-1210-CIV-DAVIS, 1999 WL 311707, at *1 (S.D. Fla. May 15, 1999).

tract consumers to their website under the guise that their sites are sponsored by or somehow affiliated" with the trademark owner.[22]

Liability may lie for linking using a number of theories. Under copyright, where no copying is involved, deep-linking allows an automatic transfer of the user to an interior web page of another website and bypassing the top-level home page. A court has compared hypertext linking to searching through a library card index to find a book in the library stacks.[23] The act of bypassing the home page may deprive the second website of revenue, because it bypasses that website's revenue-generation mechanism (such as a counter) of tracking numbers of hits. However, the law regarding deep-linking is not firmly established, thus leaving open the question of the legality of deep-linking that causes confusion to the users as to the source of the content. In deciding future cases, courts may also attempt to weigh factors such as fairness, motives, and bad faith acts.

Arriba's use of framing is distinguishable from "pure" hyperlinking (which takes the user directly to the copyright owner's site without imposition of an intervening frame), which the *Ticketmaster* court held to be permissible.[24] Courts have generally frowned upon the use of framing because the resulting framed web page may be an unlawful derivative work. Furthermore, framing may lead to a misrepresentation of sponsorship or association, and the loss or dilution of advertising potential of the framed site.

F. *Privity*

One way for ABC to clarify ownership issues as to web content is to establish privity between itself and potential owners of data or other intellectual property rights. For example, regardless of whether ABC had existing agreements with the building managers, ABC could establish a contractually binding agreement with them as to their website use by having them read and affirmatively agree to a Terms of Use Agreement, by clicking an "I Accept" button as a condition before proceeding to login (one example of a click-through agreement). With a contractual relationship, ABC may protect its database content and its intellectual property rights.[25] As one example, ABC may contractually negotiate, with the utilities, ownership and use issues for any copyrights involved, because contract rights governing databases are not preempted by copyright laws.

22. *AsiaFocus*, 1998 WL 724000, at *3.

23. *E.g.*, Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654 HLH, 2000 U.S. Dist. LEXIS 4553, at *6, 54 USPQ2d 1344, 1346 (N.D. Cal. Mar. 27, 2000) (finding no copyright violation for hyperlinking); *c.f.* Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999) (finding contributory copyright infringement by providing unauthorized links to websites displaying copyrighted text).

24. *Ticketmaster*, 2000 U.S. Dist. LEXIS at *5–7, 54 USPQ2d at 1345–46.

25. ABC may also contractually govern data privacy issues.

Requiring all users who want to use ABC's web site to sign up, or register, their accounts through ABC's web site provides a way to require these users to agree to a Terms of Use Agreement. The seminal case on the issue of *shrinkwrap* agreements, *ProCD, Inc. v. Zeidenberg*,[26] involved a consumer transaction with an end-user purchasing the product in a retail store and no other written document.[27] Shrinkwrap agreements are similar to click-through agreements in that they are each presented to a user who wants to either proceed with "opening" or "installing" software or an online function such as downloading software or webpages available through a website. The same agreement is presented to all users, and usually the parties do not meet face-to-face or personally communicate. Thus, the issue litigated in the past has been whether there has been a meeting of the minds so that a valid, and enforceable, contract is formed.

Although a click-through agreement may not be binding in some cases, these click-through agreements often will suffice to reduce a client's risk, especially if the circumstances do not indicate a contract of adhesion that unfairly burdens a user. Click-through agreements require an affirmative action on the part of the user to indicate his acceptance of the agreement.

Our scenario presented a narrow set of issues that needed to be addressed in a Terms of Use Agreement. For example, ABC's users would not be uploading or communicating lewd or obscene information in a forum such as a chat room, nor would they be bidding on items in an auction eBay-style. ABC's users would merely be logging into the website and viewing their payment histories so that they could pay their bills. Other scenarios may introduce much more complexity. Thus, reducing or minimizing risks by contract may only be partially possible with these other scenarios. But a thorough Terms of Use Agreement will provide as much certainty as possible if carefully planned.

III. Statutory Safe Harbor for OSPs

What if ABC now decides to also provide disk space to its customers to foster a sense of community spirit? The customers are permitted to upload personal web pages onto ABC's database. The questions that arise with this scenario include whether ABC is liable for infringing or defamatory material residing on their database? Further, is ABC liable for shutting down an obscene personal web page or a chat room that includes such material?

26. 86 F.3d 1447 (7th Cir. 1996).

27. A more recent case held that a clickwrap license limiting a software manufacturer's liability for damages to a licensee to the license fees paid for the software is an enforceable agreement consistent with the Uniform Commercial Code. I.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002).

A. *Digital Millennium Copyright Act*[28] (DMCA)

The DMCA provides safe harbors by protecting online service providers (OSPs) from infringing activities of third persons when that OSP is merely providing selected services. The safe harbor provides a complete bar to monetary damages and restricts the availability of injunctive relief. The services protected by the DMCA are:

- Transitory communications;
- System caching;
- Storage of information at direction of users; and
- Information location tools.[29]

The transitory communications safe harbor is available to an OSP, an entity that offers "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."[30] The safe harbor for the latter three activities is available to "a provider of online services or network access, or the operator of facilities therefor."[31] This safe harbor is also available to entities described in the OSP definition for transitory communications.

OSPs are protected from liability from certain acts are described in the statute, and it may be illustrative to discuss several cases to provide some context for those acts. In *A&M Records, Inc. v. Napster, Inc.*,[32] Napster did not qualify under the transitory communications safe harbor branch, because the transmission of infringing materials did not actually pass through Napster's computer system. The safe harbor for transitory communications are protected acts where the:

- Transmissions are not initiated by OSP;
- Transmissions use an "automatic technical process;"
- Recipients are not selected by the OSP;
- OSP does not select or modify the material;
- OSP stores a copy of the material no longer than necessary; and
- The stored copy is accessible only to an intended recipient.[33]

Moreover, an OSP is not liable for unprotected acts where a notification process is followed. In *Napster*, Napster did not take steps to inform infringing users of its termination policy.[34] The DMCA's notification process includes the following steps:

28. Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).
29. 17 U.S.C. § 512(a)–(d) (2000).
30. 17 U.S.C. § 512(k)(1)(A).
31. 17 U.S.C. § 512(k)(1)(B).
32. No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243, 54 USPQ2d 1746 (N.D. Cal. May 5, 2000), *rev'd in part on other grounds*, 239 F.3d 1004 (9th Cir. 2001).
33. 17 U.S.C. § 512(a)(1)–(5).
34. *Id.* at *7–11, 54 USPQ2d at 1748.

- Copyright owner sends written notification to OSP's agent;
- OSP expeditiously takes down material;
- OSP takes reasonable steps to notify subscriber;
- Subscriber sends counter notification to OSP's agent;
- OSP forwards a copy of counter notification to copyright owner; and
- OSP puts back material within ten to fourteen days of receiving counter notification.[35]

The other safe harbors are also detailed in the DMCA. System caching is a service provided by OSPs to retain a copy of a material so that subsequent requests for the same material may be fulfilled without having to access the original source of the material. System caching is typically done by OSPs to reduce bandwidth and wait time. The conditions for the availability of the safe harbor under system caching are where the:

- OSP did not put the material online;
- Recipient directed or initiated the transmission of cached material;
- OSP stores the material using an "automatic technical process;"
- OSP follows rules for refreshing, reloading, and updating material specified by the content provider; and
- OSP does not interfere with the content provider's technology.[36]

Storing material at the direction of users, or as commonly referred to "web hosting," will impose no liability if the:

- OSP has no actual knowledge of infringement or facts or circumstances;
- OSP acts expeditiously to take down material in response to notice;
- OSP receives no direct financial benefit; and
- OSP must have a designated notification agent.[37]

An OSP will also not be liable for providing an information location tool such as online directories and search engines if it meets the following conditions, where the:

- OSP directs users to an online location;
- OSP has no actual knowledge or awareness of infringing facts or circumstances;
- OSP expeditiously takes down the material upon notice;
- OSP receives no direct financial benefit; and
- OSP must have a designated notification agent.[38]

35. 17 U.S.C. §§ 512(c)(3), 512(g)(2).
36. 17 U.S.C. § 512(b)(1)–(2).
37. 17 U.S.C. § 512(c)(1)–(2).
38. *See* 17 U.S.C. § 512(d)(1)–(3).

Other DMCA cases include *Hendrickson v. eBay, Inc.*[39] and *ALS Scan, Inc. v. RemarQ Communities, Inc.*[40] The *eBay* court held that an Internet Service Provider (ISP) is not liable for secondary copyright infringement for listing a pirated DVD for sale under eBay's auction-type sales listings.[41] In *ALS,* the court held that the notice sent to the ISP substantially complied with the DMCA's requirements, and thus the ISP's failure to take down the material after receiving notification caused the safe harbor to be unavailable to the ISP.[42]

B. *Communications Decency Act (CDA)*[43]

The CDA provides ISPs a safe harbor from liability for tort claims such as defamation and libel. The CDA defines an ISP as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet,"[44] or a provider for an "interactive computer service."[45] The CDA also provides that an ISP is not a publisher even if the ISP took steps to remove objectionable material. In *Zeran v. AOL, Inc.*,[46] AOL was found immune from liability for defamatory postings by a third party. More recently, in *Blumenthal v. Drudge*,[47] AOL was held immune under the CDA even where it paid to distribute the publication that contained a defamatory statement.

However, as to intellectual property, ISPs will not receive safe harbor protection under either the CDA or the DMCA for infringement of trademark rights. In *Gucci America, Inc. v. Hall & Associates*,[48] the court held that Mindspring Enterprises, as a web hosting service provider, are not entitled to safe harbor for infringement of Gucci's trademark. The court stated that the CDA is not intended to "limit or expand any law pertaining to intellectual property," and that the DMCA pertains only to copyright infringement.[49]

VI. Conclusion

In our scenario, ABC should be able to significantly limit its risk exposure as it takes its business online. Our approach is to sort through ownership issues for all web content according to the type of intellectual property. To the extent ABC can, ABC should obtain a

39. 165 F. Supp. 2d 1082 (C.D. Cal. 2001).
40. 239 F.3d 619 (4th Cir. 2001).
41. *Hendrickson*, 165 F. Supp. 2d at 1088–94.
42. *ALS Scan*, 239 F.3d at 625–26.
43. 47 U.S.C. §§ 223–30 (1994 & Supp. V 1999).
44. 47 U.S.C. § 230(f)(2) (Supp. V 1999).
45. 47 U.S.C. § 230(f)(3) (Supp. V 1999).
46. 129 F.3d 327 (4th Cir. 1997).
47. 992 F. Supp. 44, 49–53 (D.D.C. 1998).
48. 135 F. Supp. 2d 409 (S.D.N.Y. 2001).
49. *See id.* at 412–13 (quoting 47 U.S.C. § 230(e)(2) (1994)).

license for content not owned, or where there is a risk that they may not have a right to include, display, distribute, or use this content. These licenses or other agreements may be executed with tenants, the utility companies, and the building managers. In most respects, agreements with the tenants may be implemented by online click-through agreements, which require each tenant to agree to particular terms and conditions.

Where risk is unacceptable in using or displaying content, ABC should remove or not use questionable content. For example, ABC should carefully examine its framing and deep-linking functions and/or whether it unauthorizedly uses any trademarks of others in its metatags. Care should be exercised to remove any use of technology where another website's intellectual property would be perceived by an ordinary user as originating from, or as affiliated with, ABC's website, when such relationship is unauthorized. ABC should also establish reasonable security measures to protect its online property from trespasses or other hackers, and to ensure that data is reasonably safe from corruption or loss. For example, ABC should implement standard firewall technology and use passwords and/or other technology to protect its online database.