Texas Wesleyan Law Review

Volume 8 | Issue 3 Article 5

7-1-2002

Protection and Enforcement of New Intellectual Property

David G. Wille

Dana Jewell

Pamela Ratliff

PROTECTION AND ENFORCEMENT OF NEW INTELLECTUAL PROPERTY

David G. Wille†
Dana Jewell††
Pamela Ratliff†††

I. INTRODUCTION

The ever-increasing popularity of the World Wide Web has prompted debate about new types of intellectual property protection. Several key advantages of the Web include (a) its global nature, (b) its relatively low cost, (c) its speed, and (d) its power. These advantages have spawned a new economy that relies upon relatively instantaneous communications of large amounts of data to large numbers of people. Unfortunately, the Web's capacity to deliver data to large numbers of people quickly and inexpensively also makes it a powerful tool for the violation of intellectual property rights on a massive scale. To complicate matters, legal doctrines need to be tested and reapplied

† Partner, Baker Botts LLP, Adjunct Professor, University of Texas School of Law, J.D. University of Michigan, M.S. University of Wisconsin (electrical engineering), B.S. University of Wisconsin (electrical engineering).
†† Associate, Baker Botts LLP, J.D. University of Michigan, B.A. Adrian College.
††† Associate, Baker Botts LLP, J.D. Vanderbilt University School of Law, B.A. Duke University.

DOI: https://doi.org/10.37419/TWLR.V8.I3.4

to new forms of conduct occasioned by the technology of the Web. Some of these new forms of conduct (*e.g.*, the use of a competitor's trademark in metatags) are not easily analyzed under existing law, and experts and laymen alike may not easily reach consensus as to what is right and what is wrong. The *Napster* and *MP3.com* cases illustrate the difficulty of drawing lines in this area.

Given the potential for widespread intellectual property violations created by the Web, it is not surprising that many have called for legislation to protect new intellectual property in the context of the World Wide Web. While the term "new intellectual property" is one that has been used frequently in the last several years, the term is a bit of a misnomer. Some use the term to refer to new rights attaching to existing intellectual property rights, such as digital performance rights granted to music copyright owners. Others use the term to refer to various forms of digital information, such as databases, web page content, and domain names. Some have called for *sui generis* intellectual property rights to protect such digital information. For example, the European Database Directive provides *sui generis* protection for databases in Europe and similar legislation has been proposed in the United States. While *sui generis* protection may be a new intellectual property right, the underlying digital information protected is not new. Databases have existed for hundreds of years (at least as the European Community defines them) and have existed in digital form for decades. Even Internet domains date back several decades. Why, then, do many refer to databases and domain names as "new intellectual property"?

Several factors have prompted calls for increased intellectual property protection. First, these digital creations have greatly increased in value in recent years. This Article will focus on databases and domain names, the two most prevalent items commonly called "new intellectual property." With respect to these items, the increase in value is apparent. Domain names were once primarily used for email communications over an Internet designed for educational and research purposes. Now that the Internet is used for commerce, the value of domain names has increased substantially. Databases have increased in value for many reasons. Databases are easier to create and link together with modern technology. Sophisticated software has increased the number of functions that can be performed using databases. The increased speed of computers and concurrent increase in the size of affordable storage media (such as hard drives and CD-ROMs) have made large databases accessible to consumers. Twenty years ago, it would have been unthinkable for an individual to have a national telephone directory database. Now, he can purchase one at a retail store for a low price and use it with a home computer.

Second, these digital creations are easier to use for illicit purposes than in the past and the rewards are bigger. The large number of top-

level domains and the ability to obtain domain names similar to domain names using famous trademarks have made it easy and inexpensive to prey upon the goodwill of others. Databases are likewise easier to use for illicit purposes. Referring to the above example, twenty years ago it would have been hard to pirate a copy of a national telephone number database. One would have needed expensive equipment to do so. If a copy was obtained, there would have been a small number of customers for it because consumers could not afford the computer equipment to use the database even if the database was obtained for free. Today, as the *ProCD* case illustrates, one can post the telephone directory on the Internet and transport it around the world in a matter of seconds. Thus, databases are (a) technologically easier to copy; (b) less expensive to copy; and (c) easier to distribute than they were previously. When these factors are combined with the increased size of the market for databases, the ability of pirates to do business over the Web anywhere in the world, and the ease of capturing data available on the Web, one has a recipe for widespread copying.

The desirability of new forms of intellectual property protection for databases and domain names is beyond the scope of this Article. Instead, this Article focuses on the protection and enforcement of intellectual property rights in databases and domain names under existing law. Because of the increased value of these assets, owners should increasingly pay attention to their protection.

II. COMPUTER DATABASES

As discussed above, the increased value of databases, the increased ease of copying, and the increased rewards for copying have prompted renewed interest in intellectual property protection for databases. Database owners will increasingly attempt to obtain better protection for their creations to maximize the return on their investment. While some call for *sui generis* protection, others believe that existing law provides adequate protection for databases. Computer databases currently may be protected from unauthorized copying by federal copyright law, trade secret law, contract law, technological measures, and common law misappropriation. Of course, all of these mechanisms will not be applicable in every instance and in some cases, none of them will.

There seems to be no precise definition of "database." One could simply view a database as a digital compilation of information arranged to facilitate search and retrieval. Different definitions of databases have been adopted in legislation seeking to create *sui generis* protection. For example, in the European Database Directive, databases are defined very broadly to include "literary, artistic, musical or other collections of works or collections of other material such as texts, sound, images, numbers, facts, and data" and to cover "col-

lections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed."[1] In contrast to this broad definition, the Collections of Information Antipiracy Act currently pending in Congress defines databases in terms of "information that has been collected and has been organized for the purpose of bringing discrete items of information together in one place or through one source so that users may access them."[2] Obviously, these definitions would apply to databases other than digital databases stored on a computer. Even assuming that computer databases deserve new forms of protection given the factors discussed above, one can question whether databases other than those stored on computers should receive additional protection. This Article will focus on computer databases.

Legislation such as the European Database Directive and the Collections of Information Antipiracy Act evidence an increasing recognition of the value of databases and the weaknesses of current protection. The value of a database lies in the compilation of the information and facts contained therein. Often the facts and information contained in a database are in the public domain, and theoretically are available to everyone. However, the data may not be easily accessible, and moreover, it is usually expensive and time consuming to gather and arrange large amounts of data in a searchable medium.

A computer database often combines the compilation of information with a search engine and user interface, which increase the speed at which the information can be searched and retrieved. Computerization of a database also allows for more complex searches of the information contained in the database. For example, a user can create search parameters to retrieve all data contained within those parameters. A computerized telephone directory user can create and run a search for all individuals who live on the streets surrounding his business in a matter of seconds; the resulting list of individuals allows him to target advertising to people who live near the business. Computerized databases are typically more valuable to consumers than paper databases because of the increased ease, speed, and parameters for searching the data.

A. *Copyright Protection for Computer Databases*

1. Protection of Databases Under Copyright Law

Federal copyright laws provide protection to authors of "original works of authorship fixed in any tangible medium of expression."[3]

1. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases.
2. H.R. 2652, 105th Cong. (2d Sess. 1998).
3. 17 U.S.C. § 102(a) (2000).

Under certain circumstances, databases and other compilations of information can qualify for copyright protection.[4] Federal copyright law protects databases if they are original (not merely copies of other databases) and if they contain some minimal degree of creativity. Most databases are compilations of facts; while the facts are not protected by copyright law,[5] the compilation may be protected if there is some degree of originality to the selection and arrangement of the facts contained therein. This is true whether the database is embodied in a computer program or in a printed book. The owner of the copyright in a database has the exclusive right to (and to authorize others to) make and distribute copies of the database and to prepare derivative works based upon the database.[6]

Prior to 1991, some databases received copyright protection under a theory known as the "sweat of the brow" theory. Under this theory, courts sometimes based copyright protection for databases on the effort required to compile the facts included in the database even though the database did not otherwise meet the creativity standard for copyright protection. However, in the 1991 decision *Feist Publications, Inc. v. Rural Telephone Service, Inc.*,[7] the Supreme Court rejected the "sweat of the brow" doctrine.[8] In *Feist*, the Court held that there was insufficient creativity in the white pages of a telephone directory to merit copyright protection.[9] The *Feist* Court predicted that most databases would contain the minimum amount of creativity required for copyright protection because the threshold level of creativity is low.[10] The Court confirmed that the facts contained in a database are not protected by copyright and can be freely used; only the author's original contributions to the database are protected.[11]

By eliminating the "sweat of the brow" doctrine, *Feist* seemingly eroded copyright protection for computer databases, but in actuality may have strengthened it by emphasizing that creative arrangements of information can be copyrightable. After *Feist*, a database creator's selection and arrangement is protected by copyright, but the facts themselves are not. By drawing the line in this manner, the Court also

4. *See id.* § 103.
5. *See id.* § 102.
6. *Id.* § 106.
7. 499 U.S. 340 (1991).
8. *Id.* at 362–63, 18 USPQ2d at 1285.
9. *Id.* at 364, 18 USPQ2d at 1285.

> The selection, coordination, and arrangements of Rural's white pages do not satisfy the minimum constitutional standards for copyright protection . . . . In preparing its white pages, Rural simply takes the data provided by its subscribers and lists it alphabetically by surname. The end product is a garden-variety white pages directory, devoid of even the slightest trace of creativity.

Id. at 362, 18 USPQ2d at 1284.
10. *Id.* at 358–59, 18 USPQ2d at 1283.
11. *Id.* at 359, 18 USPQ2d at 1283.

protected the free use of factual information for everyone. One of the criticisms that can be made of the proposed database legislation and the European Database Directive is that both measures potentially give control of the dissemination of facts to a single entity. *Feist* seems to draw a fairer line.

Later decisions have added more definition to the line drawn by *Feist* in a manner that seems to be in harmony with the Supreme Court's instructions. In *BellSouth Advertising & Publishing Corp. v. Donnelly Information Publishing, Inc.*,[12] the Eleventh Circuit held that the choice of categories for a yellow pages telephone directory was unprotectable. The Court found that BellSouth had employed "industry standards" in the arrangement of directory headings and entries, and that the businesses buying the yellow pages advertisements, and not BellSouth, decided in which category to appear.[13] In *Key Publications, Inc. v. Chinatown Today Publishing Enterprises, Inc.*,[14] the Second Circuit found that a business telephone directory very similar to the *BellSouth* directory qualified for copyright protection due to the selection of Chinese-American businesses contained in the directory. The Court ultimately held, however, that the defendant was not guilty of copyright infringement because the defendant merely appropriated some of the unprotected facts contained in plaintiff's directory and compiled them differently in his own directory.[15]

Other courts have shown that they will afford copyright protection to databases and compilations that contain some degree of originality and creativity. Some of these cases illustrate the low level of creativity required for copyright protection for databases. In *Warren Publishing, Inc. v. Microdos Data Corp.*,[16] the court held that a cable television industry database was copyrightable. While the compilation involved mostly factual information about cable television franchises, the selection and arrangement of the facts was deemed copyrightable. In *CCC Information Services v. MacLean Hunter Market Reports, Inc.*,[17] the court held that a used car valuation database was copyrightable. The court relied upon several factors to find that the database was copyrightable, including (1) the fact that valuations of used cars were based upon experience and consideration of fifteen factors; (2) the division of the national market into several regions; (3) the selection/presentation of car options (*i.e.*, the optional features a consumer could order for a vehicle); (4) the fact that price adjustments were done at 5000 mile increments; and (5) the selection of the number of

12. 999 F.2d 1436, 28 USPQ2d 1001 (11th Cir. 1993).

13. *Id.* at 1444, 28 USPQ2d at 1007.

14. 945 F.2d 509, 20 USPQ2d 1122 (2d Cir. 1991).

15. *Id.* at 514, 28 USPQ2d at 1125.

16. 52 F.3d 950, 955, 34 USPQ2d 1766, 1770 (11th Cir. 1995) (distinguishing *BellSouth*), *vacated by* 115 F.3d 1509, 43 USPQ2d 1065 (11th Cir. 1997) (en banc).

17. 44 F.3d 61, 67, 33 USPQ2d 1183, 1187 (2d Cir. 1994).

model years to include in the database.[18] Significantly, the court noted that a logical arrangement does not necessarily negate copyrightability. In *Montgomery County Ass'n of Realtors, Inc. v. Realty Photo Master Corp.*,[19] the court held that a multiple listing service database of homes for sale was copyrightable because the database included marketing puffery about various properties and used an elaborate set of abbreviations. Collectively, these cases demonstrate that the level of creativity required for copyrightability is low.

2. Registration of Database Copyrights

Although the pros and cons of copyright registration are beyond the scope of this Article, maximum copyright protection is often only available if the copyright is registered. Computer databases and compilations that meet the threshold originality requirement may be registered with the United States Copyright Office.[20] According to Copyright Office *Circular 65*, an "automated database is a body of facts, data, or other information assembled into an organized format suitable for use in a computer and comprising one or more files."[21] Computer databases may be copyrightable forms of compilations, which are "work[s] formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."[22] *Circular 65* provides instructions for the registration of computer databases with the Copyright Office. Computer databases may be registered individually or with accompanying updates and revisions.[23] Because many computer databases are continually updated and revised, the time and expense required to register the copyrights in the databases may be substantial. The Copyright Office permits group registration of computer databases on a quarterly basis, which alleviates some of the expense associated with continual registrations. The updates and revisions to a computer database may also be registered separately. Typically, fifty pages of the data records

18. *Id.* at 67, 33 USPQ2d at 1187–88.

19. 878 F. Supp. 804, 810 (D. Md. 1995), *aff'd*, 91 F.3d 132 (4th Cir. 1996).

20. U.S. Copyright Office, *Circular 65 Copyright Registration for Automated Databases* (1999), *available at* http://www.copyright.gov/circs.

21. *Id.*

22. *Id.*

23. Group registration is available for computer databases and their accompanying revisions if all of the following conditions are met: (1) all the updates or revisions must be fixed (if unpublished) or published only in machine-readable copies; (2) all the updates or revisions were created (if unpublished) or were first published within a 3-month period, all within the same calendar year; (3) all the updates or revisions are owned by the same copyright claimant; (4) all the updates or revisions have the same general title; (5) all the updates or revisions are similar in their general content, including their subject; (6) all the updates or revisions are similar in their organization; and (7) the updates or revisions, if published before March 1, 1989, bear a copyright notice naming the owner of the copyright, and that name is the same in each notice.

from the database must accompany the copyright application as deposit material. Database deposit material should be humanly intelligible, preferably printouts written in a natural language. If the deposit material is encoded, it should include a key or explanation of the code so that a copyright examiner can determine the presence of copyrightable material. Where the deposit material contains trade secrets, the Copyright Office may allow the copyright owner to block out the trade secret portions of the material or to substitute pages of code that do not contain the trade secrets. Although registration with the Copyright Office is not required for copyright protection, it is a prerequisite to a suit for copyright infringement.

B. *Trade Secret Protection for Computer Databases*

While the ease of copying databases accessible over the Web is a problem unlikely to be solved by trade secret law, trade secret protection should be kept in mind when managing certain databases. If trade secret information is contained in a database, measures should be taken to maintain trade secret status. A trade secret is information or know-how that is not generally known by the public and that gives the owner of such information or know-how an advantage over its competitors. Trade secrets contained in computer databases may be protected under certain circumstances if they are kept secret.

Even the databases most at risk from the new ease of copying (mass-marketed databases) might be able to be protected using trade secret law. It is not clear whether trade secrets contained in such computer databases, where each copy of the database is provided to the consumer under an obligation of secrecy, would be protected or whether they would be deemed disclosed and would fall into the public domain. If a database is distributed under a license agreement, there is little harm in attempting to obtain trade secret protection by putting an obligation of secrecy into the license.

Trade secret protection may be better suited for databases that are used internally within a company, such as customer lists, where the facts themselves are the valuable portion of the computer database. If the company makes reasonable efforts to maintain the secrecy of the computer database, the database may be protected from unauthorized disclosure and misappropriation under state trade secret statutes and state common law. A company that wants to protect a computer database as a trade secret may require employees and licensees having access to the database to sign confidentiality and non-disclosure agreements to ensure that the data remains a secret and does not become available to the public. Technological measures should also be taken to protect the security of the data. Moreover, access to the database should be controlled such that visitors to a company do not have access to the database.

C. *Contract Law Protection for Computer Databases*

Contract law may afford protection to computer databases that are licensed to users under circumstances where the user is in privity of contract with the database owner. In such a situation, the user may agree not to make unauthorized copies of the database or use it in some unintended manner. In many cases, computer databases are mass marketed to the public in computer superstores as prepackaged software or online as downloadable software. Other databases are accessible through the Web and used in connection with a Web browser. Users typically do not obtain complete copies of these databases but instead access them online. In either case, the database owner should seek to bind users of the database to a contractual agreement constraining use of the database. As the *ProCD* case discussed below illustrates, a database license may provide protection even where the database may not otherwise be protected by intellectual property laws.

Mass-marketed databases distributed in full to users often contain shrinkwrap or clickwrap agreements. These agreements typically provide that by opening the package, downloading the database, or using it, the user agrees to certain terms and conditions. The agreement can be written (commonly referred to as a shrinkwrap license) or can be included as part of the software such that the user needs to indicate acceptance of the terms of the agreement using a computer to use the software (commonly referred to as a clickwrap license).

The enforceability of shrinkwrap and clickwrap agreements is not clearly settled. A discussion of the desirability of their enforcement is beyond the scope of this Article. While some courts may refuse to enforce these licenses at all, the licensor can take steps to increase the potential that a shrinkwrap will be enforced, as illustrated by the contrast between the two cases discussed below.

In *ProCD, Inc. v. Zeidenberg*,[24] the Seventh Circuit Court of Appeals held that shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general, such as unconscionability.[25] In *ProCD*, the plaintiff's database was a telephone directory, which the court assumed was not copyrightable.[26] The *ProCD* software was packaged in a box that stated the software comes with restrictions contained in an enclosed license. The license was encoded on the CD-Rom disks and printed in the manual, and it appeared on the user's computer screen every time the user ran the software program. The license limited use of the software program and the telephone listings contained therein to non-commercial uses. Defendant purchased the *ProCD* software and made it available to

24. 86 F.3d 1447, 39 USPQ2d 1161 (7th Cir. 1996).
25. *Id.* at 1447, 39 USPQ2d at 1161.
26. *Id.* at 1447, 39 USPQ2d at 1161.

the public over the Internet for a fee that was less than the cost of buying the software. The Court held that the shrinkwrap license was enforceable under standard contract laws and UCC provisions, and noted that defendant had the opportunity to reject the agreement and the goods, but did not.[27]

While the agreement in *ProCD* was found to be enforceable, the court reached a different conclusion about a so-called "browsewrap" agreement in *Specht v. Netscape Communications Corp.*[28] In *Specht*, Netscape unsuccessfully tried to enforce a downloadable software license. The court did not enforce the license because Netscape simply placed a notice of the license on the same web page where the software was available for downloading. Users could download the software without reading the license or indicating their consent to it. The court distinguished the browsewrap license in *Specht* from shrinkwrap and clickwrap agreements that "require users to perform an affirmative action unambiguously expressing assent *before* they may use the software, that affirmative action is equivalent to an express declaration stating, 'I assent to the terms and conditions of the license agreement' or something similar."[29] Netscape's license "allows a user to download and use the software without taking any action that plainly manifests assent to the terms of the associated license or indicates an understanding that a contract is being formed."[30] When read together, *ProCD* and *Specht* suggest that a court will be more likely to enforce the license where there is a way for consumers to indicate their consent to be bound by the terms of the license.

One other point deserves mention with respect to contractual protection. The *ProCD* court rejected an argument that enforcement of the license under state law was preempted by the Copyright Act.[31] Preemption of state law causes of action by the copyright laws can be a problem in seeking to enforce a license agreement. The Copyright Act preempts all state causes of action which grant rights equivalent to the rights granted by the Copyright Act and extends to works that are covered by the subject matter of the Copyright Act.[32] While preemption was not found in the *ProCD* case, in comparable cases other courts have found state common law causes of action to be preempted by the Copyright Act.[33] Accordingly, there is no guarantee that a license agreement will be enforceable.

27. *Id.* at 1449–53, 39 USPQ2d at 1161–63.
28. 150 F. Supp. 2d 585 (S.D.N.Y. 2001).
29. *Id.* at 595.
30. *Id.*
31. *ProCD* at 1452, 39 USPQ2d at 1163.
32. 17 U.S.C. § 301(a) (2000).
33. *See, e.g.*, Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 41 USPQ2d 1585 (2d Cir. 1997); Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 7 USPQ2d 1281 (5th Cir. 1988); Warner Bros., Inc. v. Wilkinson, 533 F. Supp. 105, 216 USPQ 837 (D. Utah 1981).

D. *Technological Measures To Protect Computer Databases*

When possible, database creators should use technological measures to protect their databases from being copied. For example, creators of databases accessible over the Web (where a copy of the entire database is not typically provided) should use technological measures to prevent users from engaging in practices that would allow unintended uses of the data. Poor technological protection of a database may allow hackers to steal an entire database even though a website's intended use is to allow access of only a small portion of the data at any one time. In some cases, technological protection will be difficult as illustrated by the *eBay* case discussed below. Where technological measures are difficult to implement, contractual agreements may be more important, illustrating the tradeoffs among the various forms of protection available for databases.

Deep linking is one action that can sometimes be prevented with technological measures. Deep linking is a practice where one studies the structure of a web page to allow automated access to web pages and data stored on a third party website, while bypassing a home page or other intervening pages. In cases where computer databases are offered on a third party website, deep linking may allow users to bypass the clickwrap agreement and link directly to the database. Where deep linking allows users to bypass a clickwrap agreement, the enforceability of that agreement is doubtful, and protection of the database is jeopardized.

Moreover, there is uncertainty as to whether deep linking, although it may be highly objectionable to the owner of the linked website, is illegal and can be stopped through various laws. This uncertainty makes technological measures more important. In *Ticketmaster v. Tickets.com, Inc.*,[34] Tickets.com, a ticket clearinghouse, deep linked to Ticketmaster's website.[35] Tickets.com would download large amounts of information concerning upcoming events and the availability of tickets for those events. Ticketmaster objected to Tickets.com's practice and filed a complaint against Tickets.com in an attempt to stop the deep linking. The court dismissed four counts of Ticketmaster's complaint and found that Tickets.com's deep linking did not violate the Copyright Act, did not breach the terms and conditions of Ticketmaster's site that prohibited deep linking, and did not constitute unfair competition.[36] In light of this case, it is advisable for creators of online computer databases to set up their websites so that individuals cannot link to the database without first agreeing to the terms of a clickwrap license.

34. No. CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553, at *3–4, 54 USPQ2d 1344, 1345 (C.D. Cal. Mar. 27, 2000).

35. *Id.* at *3–4, 54 USPQ2d at 1345.

36. *Id.* at *10–11, 54 USPQ2d at 1347.

Deep linking is not the only way to trespass on a website. In *eBay, Inc. v. Bidder's Edge, Inc.*,[37] the defendant engaged in a different form of trespassing on eBay's website. eBay operates an online auction website, and Bidder's Edge collected information from different online auction sites which allowed online auction buyers to search for items across numerous online auctions without having to search each site individually. eBay claimed that Bidder's Edge's conduct infringed its right of privacy and that eBay had the fundamental right to stop unauthorized and harmful access to its site. eBay claimed that Bidder's Edge's conduct damaged eBay's servers and slowed down its site. In the *eBay* case, Bidder's Edge was enjoined from accessing eBay's online auction site to collect data about items for sale on eBay. The court ruled that the use of automated search programs to collect information from websites amounted to trespassing.[38] eBay's user agreement is also a useful tool for stopping this kind of activity. Technological measures would be difficult for eBay to implement because Bidder's Edge simply obtained an eBay user ID and accessed the system by programming a computer to act like an ordinary user of the system.

E. *Protection for Computer Databases Under Common Law Misappropriation*

State common law misappropriation law may be useful in protecting computer databases in limited circumstances. Where it is likely that the database lacks the minimal amount of creativity to qualify for copyright protection and therefore would not be protected by copyright law, recovery may be had under a state common law theory of misappropriation in some cases if the copyright laws do not preempt this cause of action. To succeed in an action for misappropriation, it must be shown that (1) plaintiff has made a substantial investment of time, money, or intellectual effort in creating the database; (2) defendant has appropriated the product of plaintiff's investment; and (3) defendant's appropriation has injured plaintiff. Thus, this cause of action may protect the "sweat of the brow" of the database creator.

As discussed above, where the database is properly the subject of copyright law protection, the Copyright Act preempts a claim for common law misappropriation. In a Second Circuit case, *National Basketball Ass'n v. Motorola, Inc.*,[39] the court stated that several criteria must be met in order for a misappropriation claim to survive preemption under the Copyright Act, namely, that the information must be highly time-sensitive and the defendant must be using the plaintiff's information in direct competition with the plaintiff. Thus, the

37. 100 F. Supp. 2d 1058, 54 USPQ2d 1798 (N.D. Cal. 2000).
38. *Id.* at 1069–70, 54 USPQ2d at 1807.
39. 105 F.3d at 845, 41 USPQ2d at 1589.

protection offered by the misappropriation theory is limited because not all computer databases will contain time-sensitive material. Furthermore, even appropriation by an individual who is not a direct competitor can cause substantial damage to the market for a particular computer database.

III. INTERNET DOMAIN NAMES

Domain names were created as a convenient way for humans to remember the Internet Protocol (IP) addresses used to locate other computers connected to the Internet. Without domain names to use in place of the IP number strings, most of us would find the Internet extremely inconvenient to use. However, neither the Internet nor domain names are "new." The Internet of today had its beginnings almost 40 years ago as a military command-and-control network meant to survive a nuclear war.[40] This first military communications network was called ARPANET, named after the Pentagon's Advanced Research Projects Agency, and had only four "nodes" in 1969. While ARPANET was originally intended for long-distance computing, it quickly "morphed" into a means for scientists, researchers, and other users of the time to share ideas and collaborate on projects.[41]

Thus, the Internet and domain names are not new creations. Furthermore, when domain names are considered in terms of their functional purpose—as a means of identifying and locating files on other machines connected to the Internet—domain names may appear to be unrelated to the world of intellectual property. Appearances are sometimes deceiving. With the exponential growth of the Internet and the amazing breadth of goods and services which can be purchased using only a computer and a credit card, the Internet is clearly a vibrant commercial marketplace. When trademarks are used in domain names, the worlds of intellectual property and Internet domain names collide. Unfortunately, valuable trademark rights are sometimes vulnerable in the world of domain names.

A. *Trademarks and the Problem of Distinctiveness*

A trademark is any word, symbol, or device that is used by a person or entity to identify and distinguish its goods from goods manufactured by others.[42] Well-known examples of word marks are: EXXON, KODAK, and AMERICA ONLINE. When these companies began offering goods or services in commerce under their respective marks, they acquired common law trademark rights in those marks. When

40. Numerous articles discuss the history of the Internet, including Bruce Sterling, *Short History of the Internet*, MAG. FANTASY & SCI. FICTION, February 1993, *available at* http://www.forthnet.gr./forthnet/isoc/short.history.of.internet.

41. *Id.*

42. TRADEMARK MANUAL OF EXAMINING PROCEDURE § 101 (3d ed. 2002) [hereinafter TMEP].

these companies secured federal trademark registrations for their respective marks, they gained *nationwide* rights to exclude others' use of the same or similar marks on similar goods or services.[43] Over a period of years, these and other trademark owners spent considerable sums of money to develop these marks, not only in terms of the fees required to secure the registrations, but also in terms of the marketing dollars spent to develop widespread consumer recognition in the marks.

Not all trademark owners are large companies with well-known marks. An individual trademark owner's interests in protecting its marks in cyberspace often change with the particular business circumstances at hand, including the amount of consumer recognition in any one company or mark. Large corporations like Exxon and Kodak, for example, have already established significant consumer recognition of their trademarks. These large well-established companies will be concerned with protecting their marks on the Internet (1) by ensuring that their marks are not used in different formats, such as with hyphenation or slightly different spellings; and (2) by making sure the reputations of their trademarks are not damaged by unauthorized linking to scandalous websites, for instance. For these large companies, the focus is on maintaining the integrity of their marks, while at the same time continuing to use the trademarks in a marketing context to create even more widespread consumer recognition.

In the context of the Internet, owners of trademarks that are not as widely recognized as EXXON and KODAK will have different goals in mind. For these usually smaller companies, the goal is often to (1) select a distinctive or unique trademark that stands out in the marketplace; and then (2) get as much print, media, and Internet advertising into the stream of commerce so that consumers begin to recognize the trademark and associate it with the trademark owners' products or services. In order to create a strong mark, new web businesses just starting to create goodwill in their marks will have to understand the factors that differentiate a distinctive trademark from weak descriptive marks.

The U.S. Patent and Trademark Office (PTO), differentiates between "distinctive" marks and "generic" words that are incapable of functioning as a mark.[44] To summarize, distinctive marks do not refer to the particular goods or services with which the mark is used, so that a consumer viewing only the mark (but not the goods or services) would not be informed of what the goods or services are. Examples of distinctive marks are VERIZON, MLIFE, or NIKE. Standing alone, these distinctive marks do not suggest anything about the goods or services they are connected with.

43. *See* 15 U.S.C. § 1072 (2000).
44. *See, e.g.*, TMEP § 1209.

Generic words, on the other hand, are unable to serve as a source identifier because the word or phrase is already commonly used by others to refer generally to the identified product or service. Stated differently, if a word or symbol is the common name for the goods or services with which the mark is used, it is considered "generic."[45] Examples include SOAP when used in connection with soap or detergent, LOAN when used in connection with mortgage banking services or consumer lending services, or ITALIAN FOOD when used in connection with packaged pasta or restaurant services featuring pastas and sauces. Pursuant to the Lanham Act, 15 U.S.C. § 1052(e)(1), generic words are not registrable as trademarks. These concepts of trademark law are often implicated when domain names include trademarks (for example, www.nike.com), or when domain name owners wish to acquire and assert trademark rights in their domain names.

Falling in between distinctive trademarks and generic words are descriptive trademarks. Descriptive trademarks describe some aspect of the goods or services they are connected with but are not a generic term for such goods or services. To obtain protection for a descriptive trademark, the trademark owner must prove that the trademark has obtained secondary meaning—*i.e.*, that consumers associate the trademark with the trademark owner. To obtain secondary meaning, the trademark owner must ordinarily take steps over time to create the association between the descriptive trademark and the source of the goods or services. Advertising is the most common way to do so.

Use of a domain name merely as an informational part of the domain holder's Internet address does not qualify as trademark use. That is, in order to also function as a trademark, a domain name must be used in connection with some goods or services, and not simply appear in the address line of a web browser.

> In order to qualify as a trademark or service mark, the domain name must function as a mark, that is, it must serve as an indicator of source and not merely as an informational part of an Internet web address. If the domain name functions separately as an indicator of source, the domain name may be registered with the United States Patent and Trademark Office as a trademark or service mark.[46]

Examples of registered ".COM" marks are: DOLLYWOOD.COM and GAPKIDS.COM.

Because domain names do not serve as trademarks per se, several problems arise for those attempting to establish new protection for a domain name that is not already a trademark. First, the trademark

45. *Id.* § 1209.01(c).

46. INTERNATIONAL TRADEMARK ASSOCIATION, *Differences Between Trademarks and Domain Names*, *at* http://www.inta.org/basics/ip/domnvtm.html.

owner may wish to adopt a generic term because more people may visit a website such as "loan.com" than a site with a more distinctive name. However, a website business should preferably adopt a domain name that is distinctive. A generic term will not receive trademark protection merely because ".com" is concatenated to it. Second, a website business may compromise and select a descriptive domain name. If the website business adopts a descriptive term as a domain name, then the owner will need to take steps to establish secondary meaning in the minds of consumers.

B. *Protecting Domain Names as Trademarks*

Because generic words are not protected as trademarks, there are few ways in which to protect a domain name that is comprised of a generic term. For example, if a domain name is www.loan.com, and the website associated with this website relates to banking, mortgage lending, student loans, or most any other financial-related service, it will be considered generic of those services. Accordingly, since there is no trademark protection afforded to the word LOAN in this context, the primary way to "protect" this domain name is to register it with Network Solutions and make sure to pay the annual renewal fees on time. This way, the domain name owner ensures that the domain name registration does not lapse, and cannot thereafter be registered by another. Because the domain name www.loan.com is not comprised of a trademark, it is not recognized as "intellectual property," but simply a claim of ownership in a particular piece of Internet "land." To provide better protection, the owner might seek to acquire the "loan" domain in many different countries.

There is a much more effective way to protect a domain name that includes a trademark. The trademark owner protects his domain name by registering it as a trademark with the U.S. PTO, as was done by the owners of the marks DOLLYWOOD.COM and GAPKIDS.COM. Securing a registration for the domain name in this way permits the trademark owner to protect its mark under the Lanham Act.[47] Lanham Act protection for trademarks extends to the use of the same *or similar* mark, being used on related goods or services.[48] In this way, the owner of a registration for the mark GAPKIDS.COM could bring a Lanham Act claim against a party that used or registered the domain name www.gap-kids.com. As noted above, those with descriptive domain names will need to take measures to establish secondary meaning in order to obtain a registration.

After a "domain name" trademark is registered in the PTO, the owner of the registration will be best advised to monitor and police other uses of the same or similar mark. By doing so, the trademark

47. *See* 15 U.S.C. § 1021–27.
48. *See id.*

owner protects his mark against "dilution." A mark becomes diluted when it becomes used by many different parties in connection with the same or related goods or services. When this happens, consumers begin to see the mark in connection with different parties so frequently, that the mark simply loses its capacity to distinguish one party as the source of the goods or services. Trademark owners prevent dilution from happening by enforcing their trademarks. To avoid dilution, the owner of a distinctive domain name should run searches periodically to determine whether anyone has adopted a similar domain name and should take action if that is the case.

C. *Enforcing Trademark Rights in Domain Names*

Unfortunately, it can sometimes be difficult to enforce rights in domain names, because there is no mechanism in place to preclude any individual or entity from registering a domain name which includes another's trademark. To register a domain name, all one needs to do is contact any of the domain name registries (such as Verisign, formerly known as Network Solutions, Inc.), find a domain name that has not already been registered, and submit a form along with a minimal registration fee. The domain name registries do not examine the application to determine whether another entity has rights in the mark comprising the domain name. Therefore, for example, a person or company entirely unrelated to Microsoft Corporation could successfully register the domain names www.micro-soft.com, www.microsoft co.com, www.microsoftware.com, or any other conceivable permutation and combination of the MICROSOFT mark. The only thing preventing registration of a domain name corresponding to a trademark is the possibility that the domain name has already been registered. It is not terribly difficult for a creative person to get around this minor obstacle, while it is highly unlikely that even the most vigilant of trademark owners could register domain names for every possible variation of their valuable trademarks as it would be expensive to do so.

There are a number of legal methods of enforcing rights in domain names, but most of these methods seem to put the domain name owner in a reactive position. That is, given the unregulated regime for registering domain names, the trademark owner is relegated to monitoring domain name registrations for the unauthorized use of its trademark, and then reacting to the situation by either filing a civil law suit, or an action under the Uniform Dispute Resolution Policy (UDRP). Either of these options may result in the disputed domain name being transferred to the trademark owner but each have their drawbacks. A UDRP proceeding is limited in scope to examining whether the domain name registrant should be allowed to retain the domain name, but it does not touch upon whether the domain name registrant should be allowed to use the mark in commerce and con-

texts other than the Internet. A federal civil action can resolve both the issues of registration of the disputed domain name and unauthorized use of the mark but are often prohibitively expensive.

1. Uniform Dispute Resolution Proceedings

Trademark owners may institute a UDRP proceeding to acquire a domain name that includes their trademark. The Uniform Dispute Resolution Policy was developed by the Internet Corporation for Assigned Names and Numbers (ICANN), and is incorporated by reference in the domain name registration contracts of the majority of domain name registries.[49] UDRP proceedings are most often filed in the World Intellectual Property Organization (WIPO), but may also be arbitrated by another of the arbitration bodies officially recognized under the UDRP. UDRP proceedings are generally decided by a single arbitrator, unless the trademark owner requests a three-person arbitration panel and submits the additional fee. If WIPO is the selected arbitrator, it serves the UDRP "complaint" upon the domain name registrant, who is then permitted to file an "answer."[50] Thereafter, the parties submit briefs of their respective positions, and the arbitrator(s) decide the case.

To be successful in a UDRP proceeding, the trademark owner must prove three elements: (1) that the disputed domain name is "identical or confusingly similar to a trademark or service mark" in which the trademark owner has rights; (2) that the domain name registrant has no rights or legitimate business interest in the domain name; and (3) that the domain name has been registered *and* is being used in bad faith.[51] The first element of a UDRP proceeding is generally obvious on the face of the disputed domain name and the claimed trademark. That is, the arbitration board will look at the two and see if they are identical or confusingly similar. In contrast, the second and third elements are generally more difficult for the trademark owner to prove.

To elaborate, it may sometimes be difficult to show that the domain name registrant has no legitimate business interest in the domain name. The easy case is where the domain name is "parked" with nothing more than an "Under Construction" or "Coming Soon" notice posted on the website. The situation becomes a bit more difficult when the disputed domain name resolves to a company website. Assuming the company website is legitimate—the goods or services be-

49. The UDRP can be found online at ICANN's website. THE INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, UNIFORM DOMAIN-NAME DISPUTE-RESOLUTION POLICY, *at* http://www.icann.org/dndr/udrp (last updated Feb. 5, 2002). For an example of how the UDRP is incorporated in the domain name registries' contracts, see Verisign's website, VERISIGN *at* www.netsol.com.

50. THE INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, RULES FOR DOMAIN NAME DISPUTE-RESOLUTION POLICY (1999), *at* http://www.icann.org/udrp/uniform-rules.htm.

51. *Id.*

ing offered are actually available for purchase, and the website is not a sham—it may become difficult for the trademark owner to allege that the domain name registrant has no legitimate business interest in the site. Even if the company is a small business being run out of someone's home office, it may be considered by the arbitrator to constitute a "legitimate business interest."

Similarly, the third element is sometimes difficult to prove in a UDRP proceeding—that the domain name has been both used and registered in bad faith. Again, the easy case is when the domain name registrant approaches the owner of the corresponding trademark and offers to sell the domain name. If the offering price is greater than the costs involved in registering the domain name (usually $30–50 per year), the owner of the domain name will find himself or herself on the losing side of the UDRP proceeding. This is because the UDRP arbitrators have demonstrated a pronounced tendency to protect trademark owners.

However, the facts are not always this clear. One of the more common ways trademark owners meet the "bad faith" requirement is if the domain name registrant has registered other domain names that include trademarks of other companies. This demonstrates a pattern of behavior on the part of the domain name registrant to attempt to profit from the trademarks of others by filing first for the corresponding domain names. In any event, if the trademark owner can successfully prove these three elements of a UDRP proceeding, WIPO will have the disputed domain name transferred to the trademark owner.

2. Federal Civil Litigation

If the domain name is registered as a trademark, another legal option for enforcing rights in the mark is for the domain name owner to file a federal civil action alleging infringement of the trademark under the Lanham Act, *supra*. Another federal claim that may be brought against an alleged "cybersquatter" is violation of the Anti-Cybersquatting Consumer Protection Act (ACPA), which was implemented on November 29, 1999, 15 U.S.C. § 1125(d). Required elements under an ACPA claim are: (1) that the domain name is identical or confusingly similar or dilutive of a mark that was distinctive or famous when the domain name was registered; and (2) the domain name registrant acted in bad faith in registering the domain name.[52] This second bad faith element will be met if it is successfully shown that the domain name registrant intended to divert customers, offered to sell the domain name, or warehoused multiple domain names owned by others.[53]

52. 15 U.S.C. § 1125(d) (2000).

53. For a brief discussion of the ACPA, see *Enforcement of Trademark Rights on the Internet: What Tools Are in the Toolbox?*, Kenneth R. Adamo, discussion paper from seminar delivered at the 2000 Annual Meeting of the International Trademark Association (INTA).

While these elements of the ACPA appear to be similar to the elements of a UDRP claim, the ACPA has some significant advantages over a UDRP proceeding. Notably, the only result that can come from a successful UDRP proceeding is that the disputed domain name is suspended or transferred to the successful claimant. The arbitrators in a UDRP proceeding have no power to enter an injunction, award damages, or determine which party has the right to use a mark in commerce. However, under the ACPA, remedies include injunctive relief, the defendant's profits, actual damages and costs, or statutory damages, which can be awarded between $1,000 to $100,000 per infringing domain name.[54] Secondly, the ACPA provides for *in rem* jurisdiction, so that suit can be brought against the domain name itself if the domain name registrant is unable to be located. When exercising *in rem* jurisdiction, a court can order the cancellation, forfeiture, or transfer of a domain name, but cannot award damages. Despite this drawback, the civil plaintiff has many more options under the new Anti-Cybersquatting Consumer Protection Act.

Nevertheless, civil litigation can be expensive. This expense can become prohibitive to filing a civil case if the alleged domain name/ trademark infringer has registered a domain name that is confusingly similar, but does not operate any meaningful business from which to recover damages. In this case, even if the trademark owner wins her lawsuit, the only result is that the other party loses the infringing website. In the meantime, the trademark owner has incurred considerable legal fees. Finally, if no injunction has been entered, or if the cybersquatter has not been located, there is little to prevent it from registering another slightly-altered domain name that infringes another's trademark.

As Internet law emerges on a case-by-case basis to deal with these and other issues, a number of questions remain unanswered. For example, individuals or entities in different countries may have equally legitimate rights in the same mark when it is used in their home jurisdictions. However, in light of the global reach of the Internet, it is unclear which entity would have the superior right to register and use the top-level domain (TLD) corresponding to the shared mark. That is, which party will get the ".COM" domain name? The current answer appears to be the party that registers the .COM domain first has the superior right to it. However, that answer does little to recognize the other party's legitimate rights in the mark. These and other issues will eventually be addressed as legal principles catch up to the pace of the Internet's development.

54. *Id.*

IV. CONCLUSION

While computer databases and domain names are not really "new," their value has increased substantially. At the same time, the ability of others to profit from the work of others with respect to these items has increased. These factors make conscious thought about protecting these assets more important. This Article has presented various suggestions as to how to provide protections under existing law for databases and domain names. If owners of databases and domain names put some thought into protection up front, they will create a more valuable asset over time.