DOMAIN NAMES:
UNDERSTANDING WHAT'S NEW, HOW TO PROTECT YOUR CLIENT'S PRESENCE

KARL BAYER,
DISPUTE RESOLUTION SPECIALIST
ROB HARGROVE
8911 N. Capital of Texas Highway
Suite 2120
Austin, Texas 78759
www.karlbayer.com

High Tech Litigation Megacourse
October 18-19, 2001
San Antonio, Texas
Chapter 1

KARL O. BAYER

Education

1998 The University of Texas at Austin, classes in microbiology and digital systems design
1976 University of Texas School of Law, J.D.
1973 Massachusetts Institute of Technology, M.S. (Biomedical Engineering)
1971 Rice University, B.A. *cum laude* (Electrical Engineering)

Experience

Engineering

Consulting engineer for the design of large-scale radar tracking systems
Omnibus, Founding Partner
Computer software to automate schoolbus routing

Governmental

Environmental Protection Agency
Office of General Counsel, Pesticides and Toxic Substances
U.S. Representative Kent Hance
Legislative director
State Senator Don Adams
Administrative and Legislative Aide
Texas Attorney General John Hill
Law Clerk

Legal

Karl Bayer, Dispute Resolution Specialist
Solo practice of plaintiff's personal injury and intellectual property trial law, and private mediator, arbitrator, educator, and facilitator in all areas of conflict.
Brown, Maroney, Rose, Barber & Dye, Associate
Environmental, Utility and Technology Section
Grambling, Mounce, Sims, Galatzan and Harris, Associate
Business Litigation Section

Conflict Resolution

Resolution Architects
Former Partner with Melvin E. Waxler. Conflict resolution consulting for government, private businesses and organizations, and community groups.

Publications

Co-author of articles on the regulation of genetic engineering in Vanderbilt Law Journal and Comprehensive Biotechnology; Author of papers for the State Bar of Texas, University of Texas Law School, University of Houston, South Texas School of Law, The Rutter Group, St. Mary's College of Law, and the Texas Trial Lawyer's Association on damages, product liability, jury selection, medical malpractice, pharmacist and pharmaceutical device liability, deceptive trade practices, marital torts, toxic torts, mental anguish, discovery, negotiations, alternative dispute resolution and professional responsibility.

Please read Karl's more detailed resume at **www.karlbayer.com**

Table of Contents

I. INTRODUCTION 1
A. What exactly is a domain name? How does the internet work? 1
B. Domain Name disputes 2

II. RECOVERING A DOMAIN NAME FROM A CYBERSQUATTER 2
A. ICANN's UDRP 3
1. How does it work? 3
2. With what standard does the ADR provider make a decision? 4
3. Is the UDRP fair? 5
B. The Anticybersquatting Consumer Protection Act 6
1. How does it work? 6
2. How have courts in Texas and elsewhere recently interpreted the ACPA? 7
a. *E&J Gallo Winery v. Spider Webs* 7
b. *Lockheed Martin v. NSI* 7
c. *Registral.com v. Fisher Controls* 8
d. *March Madness v. Netfire* 8
e. *PETA v. Doughney* 8
C. The Texas Anti-Dilution Statute and domain names 9

III. What if your trademark is registered by a competitor? 9
A. Websites and personal jurisdiction: *Zippo* 10
B. Aimed conduct and personal jurisdiction: *Calder v. Jones* and its progeny 11
C. Which test should apply to domain name disputes? 12
D. The problem of competitive registration and jurisdiction 13

IV. THE NEW GENERIC TOP-LEVEL DOMAIN NAMES 14

V. CONCLUSION 15

DOMAIN NAMES

I. INTRODUCTION

In the last few years, the nature of the internet domain name dispute has changed as new policies have been implemented to resolve disputes and as courts have begun to establish coherent bodies of domain-name law. A website is now considered a requirement for most businesses, large or small, and as more and more domain names are registered, more and more folks must face the unpleasant realization that someone else has registered their company's name. This paper will offer some guidance as to what someone in that situation can do. First, however, we must define a few terms and give some technical background.

A. What exactly is a domain name? How does the internet work?

Simply put, a domain name is like a street address in the internet; karlbayer.com is my web presence's domain name, and my website, my email server, and my office's internal network are all part of the domain. To many people, the term domain name just means the name of a website, but it actually refers to an entire internet presence, of which the website is an important part. It is, therefore, what one types into a browser to load a site. Technically, it is a direction computers use to download the proper html document which, when viewed by an html browser, becomes a website. Html is the language in which websites are written; it allows the integration of images and data with text and the use of hyperlinks to connect pages, among other things. The world wide web is a network of electronic files, shared by the computers on which they are located and available to the rest of us upon request. My own website, karlbayer.com, is actually a text document, written in html, which is stored on a computer at my office. When anyone types ‹http://www.karlbayer.com' into a browser (like Microsoft's Internet Explorer or Netscape's Navigator), somehow their computer knows where to find the document and how to read it. This is able to work because of a system of assigned domain names.

The string of letters a web surfer types into his or her browser, www.karlbayer.com, is known as a Uniform Resource Locator, or ?URL". This URL is actually a textual referant to an Internet Protocol or IP ?address", which is in turn a string of numbers separated by periods. When someone's browser is told to find karlbayer.com, a server, typically operated by that person's Internet Service Provider, accesses a database, which tells it that karlbayer.com may be found at the IP address: 208.188.102.185. The browser uses this information to send a request for information to this IP address, where it discovers a file which contains the data which becomes my website when interpreted by the browser. All that has really happened is that the requesting computer has downloaded and read a file from my office. The manner in which these files are located has become the subject of much high-tech bickering.

For the system to work, there can only be a single IP address for every URL. In other words, karlbayer.com can only point users to a single file. Therefore, only a single person or entity may register the karlbayer.com URL, or domain name. This was initially accomplished by only allowing one company, Network Solutions, to register domain names. Once a name was registered, no one else could register it. While there is no practical limit to the number of websites which can exist, the competition for the textual names of the sites is intense, since they are unique and significant. If someone else, say another Karl Bayer, had already registered karlbayer.com, I would not have been prevented from having a website, but I would not have been able to give it the most logical name. I could have registered karlbayerinaustin.com or karlorrinbayerjr.com, but not the simplest and best version. Any of these addresses would have refered to the same domain, 208.188.102.185, but karlbayer.com is clearly more attractive than a string of numbers.

B. Domain Name Disputes

Historically, domain name disputes fall into two general categories: competition from others who wish to use the name, and cybersquatting. Cybersquatting is a term which has been used to describe someone who registers a domain name in order to sell it to someone else, usually someone with an interest in the name; it has also been called abusive domain name registration. Distinct bodies of law have developed to deal with both types of disputes, but important questions about the law still remain unanswered. This paper will describe both types of disputes, from the perspective of someone who wishes to take back his or her domain name from someone else who has already registered it.

If someone wants a domain name that someone else has registered and the domain name is neither their own individual name or a name in which they have some sort of trademark interest, that person is out of luck. For the most part, domain name registration continues to be on a first-come, first-serve basis. If I just have a great idea for a website, such as cheapusedcars.com, there is nothing I can do to develop the site, since it is not available for registration. My only option is to purchase the domain name from its owner. Therefore, this paper's discussion will focus on procedures and causes of action available to trademark owners seeking to assert their rights in trademarks registered as domain names by others.

II. RECOVERING A DOMAIN NAME FROM A CYBERSQUATTER

In 1998, in response to growing dissatisfaction with the quasi-governmental nature of internet management, open competition between domain name registrars was permitted, and for the first time Network Solutions, Inc. was not the only domain name registrar. *See Management of Internet Names and Addresses, 63 Fed. Reg. 31741* (June 10, 1998), also known as the ?White Paper". A domain name registrar is a company or entity with which someone has registered a domain name, such as Network Solutions or Register.com. The Federal Government, in response to a number of concerns, including the conflict between trademark rights and domain name registration, proposed that in addition to allowing for competition between domain name registrars, a system of domain name dispute resolution should be implemented. *Ibid.* In October 1998, the Internet Corporation for Assigned Names and Numbers (?ICANN") was formed. *See* <http://www.icann.org/general/fact-sheet.htm>, last visited 9/17/01. As part of its mandate, ?ICANN has been recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system." *Ibid.*

The ?White Paper", which summarized the more than 430 comments to the government's original proposal to de-monopolize domain name registration, acknowledged the difficulties facing domain name disputants. *White Paper,* at 31746-7. The very nature of the internet invites conflicts between people who could be anywhere in the world, so questions of jurisdiction, venue and convenience allowed for abuse of trademark rights. *Ibid.* Therefore, the White Paper suggested, and ICANN implemented, a system whereby companies authorized to sell and register domain names must agree to abide by a Uniform Dispute Resolution Policy (?UDRP") to handle domain name disputes. *Ibid.* This uniform policy, adopted by all registrants, would be administered wholly over the internet, and would therefore allow trademark holders to assert their rights throughout the world. Importantly, the UDRP was never designed for infringement claims between competitors: ?where legitimate competing rights are concerned, disputes are rightly settled in an appropriate court." *Ibid*., at 31747.

On December 1, 1999, ICANN's UDRP, which is an arbitration agreement signed by all domain name registrants, opened for business. *Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy*, at <http://www.icann.org/udrp/udrp-schedule.htm>,

last visited 9/17/01. It has become one of the simplest and easiest ways a trademark owner can contest a domain name registration, and I will discuss it at length below.

At about the same time in late 1999, President Clinton signed into law the Anticybersquatting Consumer Protection Act (?ACPA"), which amended the Lanham Act to offer a remedy to trademark owners whose trademarks are registered by others (cybersquatters) as domain names. *15 U.S.C. §1125(d)*. Like ICANN's UDRP, the ACPA makes actionable conduct which would not normally constitute infringement or dilution under existing federal trademark law. It is also aimed against cybersquatting, or bad faith domain name registration, so it too was not intended to apply to a legitimate dispute between folks who both plan good-faith use of a domain name. The UDRP and ACPA are, however, powerful weapons against cybersquatting which were intended to make pursuing bad faith registration easier and cheaper.

A. ICANN's UDRP

1. How does it work?

The UDRP is essentially an arbitration agreement between domain name registrars. *Rules for Uniform Domain Name Dispute Resolution Policy*, found at <http://www.icann.org/udrp/udrp-rules-24oct99.htm>, last visited on 9/17/01 (?UDRP Rules"). During the period before ICANN's creation and the UDRP Rules approval process, internet users debated different ways to protect trademarks. *Improvement of Technical Management of Internet Names and Addresses; Proposed Rule*, 63 Fed. Reg. 8826 (February 20, 1998), also known as the ?Green Paper". The Green Paper, which preceded the White Paper and called for comments during the rule making process, discussed a number of ways registrars could protect trademarks. *Ibid.*, 8829-30. Significantly, a number of stronger methods were discussed than were eventually implemented, such as a requirement that registrants or even registrars perform a trademark search before allowing a registration. *Ibid.*, 8830. Ultimately, no requirement that domain names ?clear" a trademark search was added to revised domain name registration procedure, but the UDRP was designed to allow for convenient resolution of disputes.

The UDRP is an agreement between registrars and ICANN, and not between the registrants and ICANN. *UDRP*, 1. Therefore, when a person or an entity seeks to challenge a domain name registration, often times the alleged cybersquatter does not respond at all. *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, Professor Michael Geist, available at <http://aix1.uottawa.ca/~geist/geistudrp.pdf>, last visited 9/17/01. A UDRP complaint is initiated when a complainant sends the complaint to one of four ICANN-approved ADR providers. *UDRP Rules*. As of the date of this writing, four firms were approved by ICANN to provide arbitration services. *ICANN website*. The World Intellectual Property Organization (?WIPO") developed much of the domain name dispute process, largely in response to international criticism that the White Paper called for United States intellectual property law to become ?the law of the internet". *White Paper*, at 31746. As of July 7, 2001, WIPO maintained the largest market share of UDRP complaints, handling 58% of the UDRP caseload. *Geist*, at 6. The four providers each have their own procedural rules, but all procedures must, of course, abide by the general structure of the UDRP Rules.

Once the ADR provider receives the complaint and determines it to be procedurally sound, the provider forwards the complaint to the registrant for a response. *UDRP Rules*, 4. This seemingly bland procedural point may in fact prove to be critical. The complainant and the ADR provider forward the complaint to the alleged cybersquatter based on the information the registrant provided to the registrar at the time of the domain name registration. The ability to locate cybersquatters was a much-debated issue during the period between the Green Paper and the White Paper, and it was resolved by the use of the whois system. *White Paper*, at 31746. The whois system is simply a database that tells anyone

who asks who registered a particular domain name. The database used to be central, but opening the registration industry up to competition has meant the creation of a whois database for each registrar. Now, to discover who owns a domain name, one can perform a search on internic.net which reveals the registrar that registered the name, and then one must search that registrar's own database to discover who actually owns the site.

When anyone purchases and registers a domain name, that person is required to submit whois information for inclusion into the database, and it is this information which is used to contact the domain name registrant when a UDRP complaint is made. Since cybersquatters may not always be forthcoming, this system of voluntary compliance does not ensure the accuracy of their contact information. In the past, this feature of cyberpiracy was a problem for trademark holders, who found it difficult to confront registrants once the registrants discovered that a quick sale was not possible. *Green Paper*, at 8829. Now, however, the URDP Rules provide that should the domain name registrant not provide a response to the trademark holder's complaint, the ADR provider should decide the dispute based on the complaint alone. *UDRP Rules*, 5(e). Therefore, while a cybersquatter may attempt to ignore threats or negotiations from trademark holders, if she or he ignores the UDRP complaint, the result is an almost certain loss of the domain name. *Geist*, 19-20.

Assuming the domain name registrant does properly receive the complaint, he or she has 20 days in which to file a response with the ADR provider. *UDRP Rules*, 5. At this point, the respondent may request that a three-member arbitration panel, rather than a single arbitrator, handle the complaint, providing that the complainant did not request a three-member panel at the outset. *Ibid.* Commentators have claimed that this decision is a critical one to ensure a fair proceeding, as domain name registrants statistically fare much worse with single arbitrators (more on this later). *See, for example, Geist.* All of this information is sent to and from the ADR provider via e-mail, and there is no hearing or teleconference during the proceeding. *UDRP Rules*, 13. The arbitrator or panel of arbitrators makes a decision based upon written material submitted by the parties, and by agreement the domain name registrar is bound by the decision. *UDRP Rules*.

2. With what standard does the ADR provider make a decision?

A complaint under the UDRP, according to the UDRP Rules, must contain and describe three elements to be successful:

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and
(2) why the Respondent (domain-name holder) should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and
(3) why the domain name(s) should be considered as having been registered and being used in bad faith. *UDRP Rule 3(b)(ix)*.

Again, these elements establish the UDRP as a useful procedure only for trademark holders dealing with alleged cybersquatters. Element (3), bad faith, is defined by the actual UDRP, and not the UDRP Rules:

Evidence of Registration and Use in Bad Faith. For purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant

who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, providing that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting a competitor; or

(iv) by using the domain name, you have intentionally attempted to distract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your website or location or of a product or service on your web site or location. *UDRP*, paragraph 4(b).

Therefore, the UDRP reflects the White Paper's mandate that it is not to be used as a device to resolve disputes between ?legitimate competing rights". *White Paper*, 31747. Put another way, if a domain name holder registers the domain name to actually compete with the trademark holder, he or she may be infringing on the trademark, but he or she is not a cybersquatter.

3. Is the UDRP fair?

Since the UDRP was adopted and implemented, a number of web sites and groups have complained bitterly that it ?is systemically biased in favor of trademark holders". *Geist*, at 2. Michael Geist, who is a an Assistant Professor of Law at the University of Ottawa, has conducted statistical analysis of all decisions made under the UDRP as of July 7, 2001, and his report is frequently cited by UDRP critics. He concludes that the process is an unfair one and should be changed, most significantly by requiring three-member arbitration panels. *Geist*, 26-7. However, Prof. Geist and the other critics seem to proceed from a problematic starting point. If they are correct and the UDRP does favor trademark holders, is this not the point of the UDRP? The policy was specifically implemented to protect trademark rights, and if complainants can show that they do in fact have such rights, should they not expect to win?

Much of the UDRP criticism has focused on the concept of reverse domain name hijacking, which is a term used to describe a large company's use of threats to take a domain name from the hardworking small businessperson who registered it. *Homepage of the Domain Name Rights Coalition*, <http://www.netpolicy.com/mainindex.html>, last visited 9/17/01. *See also Registral.com, L.L.C. v. Fisher Controls Int'l, Inc., et al.*, 2001 U.S. Dist. LEXIS 10002 (S.D. Tex., 2001). The Domain Name Rights Coalition, according to their website, is a group which ?represents the interests and views of entrepreneurs, small businesses and individuals on the Internet". *Ibid.* The Coalition urges domain name registrants to fight trademark owners for the domain names, and sites like its own are frequently found at contested domain names. *Registral.com; E&J Gallo Winery v. Spider Webs Ltd., et al.*, 129 F. Supp. 2d 1033, 1040-1 (S.D. Tex. 2001). In other words, when an unsuspecting internet browser looks for a winery web site at the URL ernestandjuliogallo.com, he or she finds instead a web site discussing in detail the way a major corporation is out to get Texas entrepreneurs. *Gallo*, at 1039.

Many of these reverse domain name hijacking complaints are made by rather blatant cyber-squatters; the *registral.com* case involved a company which used sophisticated software to scan the internet registrars for large companies whose

domain name registrations had mistakenly expired, so that they could be purchased and re-sold. *Registral.com*. However, the underlying concept is not wholly without merit, as more technologically sophisticated corporations have been known to attempt to secure any domain name which contains even a reference to their trademarks. But, these voiced concerns with the UDRP still seem tenuous, since the UDRP continues to apply only to bad-faith registration. A legitimate, potentially infringing registration for the purpose of actual use, as opposed to sale, is still bound by trademark law, and not ICANN and the UDRP.

Finally, a number of groups have emerged which are critical of the manner in which ICANN itself is run. *See, for example, ICANN Watch*, <http://www.icannwatch.org>, last visited 9/17/01. ICANN Watch compiles news articles about the management of the internet and posts editorials about ICANN policies. *Id.* The group's central complaint seems to be that the manner in which ICANN board members are selected has not comported with promises made by the corporation at its inception. *Id.* Internet advocates fought for a policy which opened domain name regsitrars to competition and which represented a step away from governmental involvement, and yet they complain bitterly that the private company established in response to these complaints is not subject to any sort of review. *Id.*

Trademark holders may also question the fairness of the UDRP. As of mid-September, 2001, the cheapest UDRP arbitration fee was $950.00 for a single disputed domain name with the National Arbitration Forum, one of four ICANN approved providers. *NAF Supplemental Rules*, <http://www.arbforum.com/domains/domain-rules020101.asp>, last visited 9/18/01. Therefore, the UDRP itself sets the baseline value for a small-time cybersquatter at roughly a thousand dollars. Since the complainant (domain name holder) pays the fee in its entirety, a cybersquatter can make a quick grand by registering a domain name which he or she knows will be contested, and then selling for the price of an arbitration. Economically, a domain name holder, even if he or she has a slam-dunk UDRP case, should pay this amount rather than undergo the hassle, uncertainty and expense of a complaint. It is also important to note that the UDRP proceeding is the easiest, cheapest and most domain-name-holder-friendly option for a domain name dispute, so at some level it seems impossible to prevent a cybersquatter from making at least $1000, assuming that the trademark holder's goal is the quick acquisition of the domain name.

B. The Anticybersquatting Consumer Protection Act

1. How does it work?

The UDRP is useful and convenient as it is administered electronically. Since the UDRP is not a court proceeding, and since UDRP filings can be done via email, the typical geographic problems which pervade domain name disputes do not hamper administration of the UDRP. But, some domain name disputants may feel dis-satisfied by the UDRP's only remedy: transfer of the domain name. The ACPA serves to fill a gap between the UDRP and conduct which is something more than mere cybersquatting and for which remedies are available in traditional trademark law.

The ACPA is an amendment to the Lanham Act which makes conduct similar to bad faith as described by ICANN actionable. *15 USC §1125(d).* Like the UDRP, the ACPA requires both a trademark and bad faith on the part of the domain name registrant. *Id.* The complete text of the ACPA, which contains the ACPA's definition of ‹bad faith', is included as Appendix A to this paper. Significantly, the ACPA allows a trademark holder to recover damages from a registrant as he or she would for any violation of the federal trademark law. *15 USC §1117.* A court also has the discretion to impose a fine of up to $100,000.00 for each violation if the court sees fit. *15 USC §1117(d).*

Again, unlike the UDRP, the ACPA simply expands a statutory cause of action to include cyber-squatting, which means that, as a lawsuit, it invokes due process protections for registrants which may not exist in the UDRP. While a trademark owner

can make a UDRP complaint against anyone anywhere, an ACPA party must navigate complex issues of jurisdiction and venue which the internet makes rather difficult. However, since the UDRP does not prevent a subsequent lawsuit, a domain name holder may choose to use the cheaper and simpler UDRP first, and then proceed with an ACPA lawsuit; conversely, registrants have used the ACPA as a means of appealing an adverse ruling from a UDRP arbitration panel. *Lockheed Martin Corp. v. Network Solutions, Inc., et al.,* 141 F.Supp2d 648, 652 (N.D. Tex. 2001).

2. How have Courts in Texas and elsewhere recently interpreted the ACPA?

a. *E&J Gallo Winery v. Spider Webs*

On January 29, the U.S. District Court for the Southern District of Texas offered an interpretation of the ACPA in a cybersquatting case described briefly above. *E&J Gallo Winery*. The *Gallo* registrant-defendant, like the defendant in the *Registral.com* case, was a clear-cut cybersquatter who had registered nearly 2000 domain names as of January 2001. *Gallo*, at 1035. As an anticipatory defense to the suit, the registrant posted a website decrying ?the risks of alcohol use and alleged misrepresentations made by corporations." *Id.* This website is apparently still operated by a *Gallo* defendant, a Houstonian named Steve Thumann. *SpinTopic.com - Your Voice in the CyberWorld!*, <http://www.spintopic.com/>, last visited 9/25/01. The *Gallo* registrant's conduct is clearly, according to the court, the kind of conduct the Senate intended to stop with the ACPA, despite Thumann's use of the site to arguably advance a political message. *Gallo*, at 1046.

The registrant's chief argument against the invocation of the ACPA seems to be that the ACPA is unconstitutional as overbroad and as an unlawful taking. *Id.*, at 1047. While the court offers citations to other opinions from around the country upholding the constitutionality of the ACPA, the opinion does not provide any analysis of the constitutional issues raised by Mr. Thumann. *Id.*, at 1047. However, it seems safe to conclude, perhaps from the lack of constitutional arguments in subsequent Texas ACPA opinions, that the ACPA is on firm constitutional footing in Texas federal courts.

b. *Lockheed Martin v. NSI*

The U.S. District Court in Fort Worth filed its opinion in the *Lockheed Martin* case on May 1, 2001. The case was an important one, as Lockheed Martin, whose Skunk Works trademark had long been the subject of domain name disputes, had sued Network Solutions, Inc. under the ACPA only a few months after President Clinton signed the Act. *Lockheed Martin*, at 649. This choice of defendants was significant as Network Solutions is not a cybersquatter, but is instead one of the largest domain name registrars in the world. The court ruled that the ACPA did not apply to registrars absent bad faith on the part of the registrar, as opposed to the registrant. *Id.*, at 654-5. According to the court, a domain name registrar that just registers domain names for cybersquatters does not meet the ACPA's bad faith standard. *Id.*

While the *Lockheed Martin* case seems like a simple decision, it is a critical one, since a cause of action against registrars would have subverted the UDRP/ACPA scheme for contending with the problem of cyberpiracy. Lockheed Martin apparently urged that the Court impose upon registrars a duty to pre-screen all domain name registrations for potential trademark violations. *Id.*, at 655. Such a screening process would have radically changed the domain name registration process since, as the Court notes, ?ninety percent of the time, the registration process does not involve human review or participation". *Id.* at 651. To have ruled otherwise, the court would have, at least in Texas, required the type of regulatory system which every internet stakeholder, from the government to registrars to ‹entrepreneurs', has sought to avoid.

c. Registral.com v. Fisher Controls

The District Court in Houston weighed in on the ACPA in late June. *Registral.com v. Fisher*

Controls Int'l Inc., 2001 U.S. Dist. LEXIS 10002 (S.D. Tex. 2001). The registrant in the *Registral.com* case seemed particularly heinous: registral.com was a Texas L.L.C. which operated software that probed domain name registries seeking well-known trademarks whose corresponding domain name registrations were about to expire. *Id.*, at 4-9. If a company mistakenly let their domain name registration lapse, Registral.com would grab the domain name and then attempt to re-sell it to the company. *Id.* When a UDRP arbitration panel held that Registral.com had violated the UDRP by registering fisher.com, Registral.com sued Fisher Controls as a means of appealing the decision. *Id.*, at 7-8, note 1. The Court was unimpressed with Registral.com, which, at various times, accused Fisher Controls of reverse domain-name hijacking on a website at fisher.com and actually registered as domain names the names of Fisher's attorneys. *Id.*, at 11. Though it makes for an interesting story, the *Registral.com* adds little to the ACPA caselaw, since the registrant rather clearly met most of the ACPA's bad faith standards. *Id.* at 24-5.

d. *March Madness v. Netfire*

A couple months later, in August of 2001, the Federal District Court in Dallas handed down a decision on cross motions for summary judgment in a case which involved the ACPA. *March Madness Athletic Assn. v. Netfire, Inc., et al.*, 2001 U.S. Dist. LEXIS 12426 (N.D. Tex. 2001). The *March Madness* case was factually quite complex, and the Defendant argued that this complexity meant that the ACPA did not apply to his registration, since he ?had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful". *March Madness*, at 36, *citing 15 USC §1125(d)(1)(B)(ii).* In other words, the defendant argues that since the ownership of the March Madness trademark was contested when he registered marchmadness.com, the registration of the domain name could not have been in bad faith. *Id.* The court was not impressed with this argument, and they set down a rule for the ACPA which is not dependent on what a registrant may or may not know at the time of registration: ?the provision should be interpreted to mean that a person acts in bad faith when using a domain name that is identical, confusingly similar to, or dilutive of a mark that was distinctive or famous at the time it was registered, regardless of what that person knew at the time of registration." *Id.*, at 38. While it should be noted that this opinion was in response to the registrant-defendant's motion for summary judgment, Judge Buchmeyer's rule is another example of Texas courts' willingness to strongly apply the ACPA against alleged cybersquatters.

e. *PETA v. Doughney*

On August 23, the Fourth Circuit handed down its decision in what has become a fairly famous case involving a well-known cybersquatter and a group of rather vocal vegetarians. *People for the Ethical Treatment of Animals v. Doughney*, No. 00-1918 (4th Cir., 2001). The domain name peta.org had been the subject of controversy since a cybersquatter first registered it in 1995. *Id.*, at 3. The registrant, a Michael Doughney, originally created a website titled ?People Eating Tasty Animals" at the domain, and during the period from the domain's initial registration until the Fourth Circuit's August opinion Mr. Doughney and the People for the Ethical Treatment of Animals (?PETA") fought a heated and public battle over the domain. *Id.; see also People Eating Tasty Animals* <http://www.mtd.com/tasty/>, last visited 9/25/01; *People for the Ethical Treatment of Animals*, <http://www.peta.org/>, last visited 9/25/01. Since the 1995 registration pre-dated the UDRP, PETA and Mr. Doughney's battle over the domain name was hampered by the previous domain name dispute policy, which simply placed peta.org in escrow until the dispute could be resolved. *PETA v. Doughney*, at 4.

PETA's original lawsuit also predated the ACPA, but a later motion for summary judgement invoked the new legislation, and the Fourth Circuit's opinion offers further analysis of the statute. *Id.* at 10. Doughney, like the *March Madness* registrant, attempted to invoke the ‹safe harbor' of

§1125(d)(1)(B)(i). *Id.*, at 13. According to Doughney, since he thought he had a First Amendment right to parody PETA, he ?believed and had reasonable grounds to believe that the use of the domain name was fair or otherwise lawful". *15 USC §1125(d)(1)(B)(ii); PETA v. Doughney* at 14. The Fourth Circuit, affirming the District Court, held that despite Doughney's beliefs, there was no reasonable ground on which he could stand. *Id.* A defendant, in the Fourth Circuit, who registers what he knows to be someone else's trademark, simply cannot find shelter from the ACPA in the safe harbor provision. *Id.*, at 15. This rule, if combined with the rule expressed by Judge Buchmeyer in *March Madness*, would effectively eliminate many arguments cybersquatters might make against the implementation of the ACPA; there would be no conceivable justification for registering someone else's trademark, at least registering it for the purpose of selling it or preventing the trademark owner from using the domain. The safe harbor provision, it would seem, is designed to allow a registrant who has a good faith argument for use of the domain to escape ACPA liability. This argument, of course, would then invoke traditional trademark law, as it would have to be a dispute between competing claims to a trademark.

C. The Texas Anti-Dilution Statute and domain names.

Texas trademark law contains a provision whereby a trademark holder may seek an injunction to prevent ?an act likely to injure a business reputation or dilute the distinctive quality of a mark." *Tex. Bus. & Com. Code §16.29.* Broader than federal dilution law and the ACPA, courts have interpreted the Texas Anti-Dilution Statute to give trademark holders a powerful tool with which to prevent registrants from using their marks as domain names. *See, for example, Gallo*, at 1041-2. According to the *Gallo* court, all that is required for an injunction is that a trademark holder be unable to use the mark as a domain name. *Id.* Indeed, as the Texas Third Court of Appeals described domain name disputes in early August, ?when a party registers another's trademark as a domain name, the trademark owner is effectively enjoined from using its own trademark to identify its own goods and services on the Internet. *Horseshoe Bay Resort Sales Co. v. Lake Lyndon B. Johnson Improvement Corp.*, 2001 Tex. App. LEXIS 5355, at 25-6 (Tex. App. - Austin 2001). Thus, in order to prevail under the Texas Anti-Dilution statute, neither bad faith, as described by the UDRP and the ACPA, nor traditional trademark infringement is required.

While the Texas Anti-Dilution Statute is seemingly the most powerful weapon yet for protecting trademarks from being registered as domain names, its application is necessarily limited by several factors. First, the only remedy available under the Texas statute is an injunction, so damages are not available. Since using the statute requires filing a lawsuit, in most cases a UDRP proceeding would make more sense, as the UDRP would require less expense. However, in a case where a trademark is registered by a non-cybersquatter, that is, by an actual competitor who claims a right to the domain name, the Texas Statute would be a good tool to use, since the UDRP by design is not well-equipped to deal with non-cybersquatters. Perhaps the biggest obstacle preventing widespread use of the Texas Statute is the fact that it is a Texas statute. Unless the domain name registrant is a Texan, the statute provides little, if any help (more on personal jurisdiction later). However, if the registrant is a Texan, it certainly makes sense to include a claim under the Texas statute in a suit to recover the domain name.

III. What if your trademark is registered by a competitor?

At first blush, this second type of domain name dispute seems simpler, since it is one for which we should not need much new law. Trademark law should be equipped to deal with the situation where a mark is used against its owner as a competitor's domain name. Indeed, the ACPA was seen as a necessary amendment to the Lanham Act since much cybersquatting behavior, while irritating, did not rise to the level of trademark infringement.

When the dispute does rise to the level of infringement, however, the ACPA and the UDRP are designed to take a back seat to traditional trademark law. Again, as was noted in the White Paper, ?where legitimate competing rights are concerned, disputes are rightly settled in an appropriate court". *63 Fed. Reg. 31741, 31747* (June 10, 1998).

This paper will not attempt to discuss all the details of the current state of the Lanham Act as it relates to internet domain names. Again, this paper assumes the threshold question, that a protectable trademark does indeed exist. Given this assumption, the registration of the trademark by a non-cybersquatting competitor is grounds for an action for trademark infringement or trademark dilution. The manner in which the action is brought, and more accurately, where the action is brought, is what seems to be the most intriguing question, and it is the question which will command the most space here.

A. Websites and personal jurisdiction: *Zippo*.

If a Texas client feels that his or her trademark has been registered as a domain name, an early question to ask should be: can we haul the registrant into a court, federal or otherwise, in Texas? This question has been and continues to be the subject of much writing. Unfortunately, the quick answer, if the registrant lives or operates elsewhere, is that it is tough to call.

Since the internet allows people to infringe upon trademarks from all over the world, individuals and companies have long been concerned that establishing a web presence will subject them to jurisdiction all over the world. Given courts' interpretation of Texas' long-arm statute, a Texas court may exercise personal jurisdiction over a non-resident defendant in any case in which such jurisdiction would not violate the Due Process Clause of the Fourteenth Amendment. *David Mink v. AAAA Development, L.L.C.*, 190 F.3d 333, 335-6 (5th Cir. 1999). The Due Process test is met if the defendant is found to have established ‹minimum contacts' with the forum state, and the exercise of personal jurisdiction does not offend ?traditional notions of fair play and substantial justice". *Id, citing Latshaw v. H.E. Johnston*, 167 F.3d 208, 211 (5th Cir. 1999), *quoting International Shoe Co. v. State of Washington*, 326 U.S. 310, 316, 66 S. Ct. 154 (1945).

The question, then, becomes whether or not a web presence in a state is a minimum contact. The Fifth Circuit, like several other circuits, has adopted the test established by a District Court in Pennsylvania for determining if a particular website establishes minimum contacts. *Mink* at 336, *citing Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D. Pa. 1997). Therefore, in Texas, we use what is known as the *Zippo* test, or the ‹sliding scale' to attempt to answer the personal jurisdiction question.

The registrant in the *Zippo* case was not a cybersquatter, but was instead a company based in California which provided an internet news service to its subscribers. *Zippo*, at 1121. The famous Zippo lighter company, based in Pennsylvania, discovered that they could not establish a web presence at zippo.com, and they sued Zippo Dot Com in Pennsylvania. *Id.* After giving a general background on personal jurisdiction and the unique problem posed by the internet, the *Zippo* court establishes what has become their fairly famous ‹sliding scale test'. *Id.*, at 1122-5. According to the court, ?the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." *Id.* at 1124. The court describes the ends of the spectrum, that is cases where jurisdiction is clearly proper and improper, as cases where a defendant enters into a contract to transmit files over the internet and cases where a defendant merely posts a passive website which only offers information and has no potential for interactivity. *Id.* In the middle are the cases where information is exchanged but contracts are not formed. *Id.* ?This sliding scale", according to the court ?is consistent with well developed personal jurisdiction principles". *Id.*

After the court establishes the scale and

discusses cases which fall at various points on the scale, the problem with the *Zippo* scale becomes apparent: many cases, if not most, will fall somewhere between the two well-established end points. *Zippo* ultimately tells courts that between the two obvious cases there is room for judgement calls on a case-by-case basis. The *Zippo* facts themselves supported personal jurisdiction, because Zippo Dot Com sold approximately 3000 passwords to Pennsylvania subscribers to its news service. *Id*., at 1126. In the Texas case which adopted the *Zippo* rule, the Fifth Circuit found that a website which provided information and forms to users but did not allow for actual interactivity did not support personal jurisdiction. *Mink*, at 336-7. For a more detailed critique of *Zippo* and a number of suggestions for better handling the question of personal jurisdiction and the internet, particularly on a global, rather than just a national, level, two California attorneys presented a paper at a joint Berkley/University of Texas conference on computer law which is currently being updated for publication. Michael Traynor & Laura Pirri, *Personal Jurisdiction and the Internet: A Return to Basic Principles*, COMPUTER AND TECHNOLOGY LAW CONFERENCE, Berkeley Center for Law & Technology and The University of Texas School of Law, June 28, 2001.

Since *Zippo*, federal courts in Texas have applied the sliding scale to a number of websites. This paper will not review all these decisions, since although some of them involve domain name disputes, the cases do not necessarily specifically apply to domain name disputes, for reasons which we will discuss later.

B. Aimed Conduct and Personal Jurisdiction: ***Calder v. Jones*** and its progeny

The *Zippo* sliding scale is the test Texas courts must now use to decide if a website on its own subjects the site owner to a Texas court's personal jurisdiction. However, a different test exists which, while it does not specifically apply to websites, may well be better-suited for domain name disputes. *See Traynor & Pirri*, at 14 (while Traynor & Pirri offer a good national discussion of these issues, they do not spend significant time on Texas-specific cases and issues). In 1984, the United States Supreme Court allowed a federal court in California to exercise personal jurisdiction over a Florida magazine in an action for libel. *Calder v. Jones*, 465 U.S. 783, 104 S.Ct. 1482 (1984). The magazine's editor challenged jurisdiction on the basis that all of his actions which formed the basis of the suit occurred in Florida, and that he had no significant contacts with California. *Id.* at 786, 1485. After recognizing that this was a question of specific, rather than general, jurisdiction, the Court notes that ?California is the focal point both of the story and of the harm suffered". *Id.* at 788-9, 1486-7. The Supreme Court ?hold[s] that jurisdiction over petitioners in California is proper because of their intentional conduct in Florida calculated to cause injury to respondent in California." *Id.* at 791, 1488. In other words, the Supreme Court allows what is known as the ?effects test" to convey personal jurisdiction when activity in one state causes actionable conduct in the different forum state.

This ?effects test", as we will see, has been the subject of much discussion since 1984, and its application to domain name disputes is still uncertain, at least in Texas. However, it is an important part of the discussion because, unlike *Zippo*, it is not an internet-specific jurisdictional test. It does not require courts to make judgements as to the degree to which a web site is interactive. If *Zippo* decisions are based on the nature of the web site, effects decisions would be based on the nature of the registration.

A few years after *Calder v. Jones*, the 5th Circuit took strides towards reigning in the possible extension of the effects test to provide for specific jurisdiction in any case of an intentional tort. *Southmark Corp. v. Life Investors, Inc., et al.*, 851 F.2d 763 (5th Cir. 1988). The *Southmark* plaintiff argued that *Calder v. Jones* stood for the proposition that ?since there is *prima facie* evidence that USLICO committed an intentional tort against Southmark in Texas with knowledge that Southmark is a Texas resident", the Texas court had personal

jurisdiction over USLICO. *Southmark*, at 772. The Fifth Circuit did not accept this interpretation, asserting instead that ?the fact that Southmark has its principal place of business in Texas is, as the district court put it, a mere fortuity". *Id.*, at 773. Therefore, at least in the 5th Circuit, it is clear at this point that something more than damage to a company which has effects in Texas is needed to convey personal jurisdiction.

The Fifth Circuit distinguished between mere forseeability and the intended effects of contact with a forum state in a recent decision involving a cause of action for fraud. *Wien Air Alaska, Inc. v. Brandt*, 195 F.3d 208 (5th Cir. 1999). The Court made an important distinction between a tortfeasor's being able to foresee that his tort will cause injury in Texas, and a tortfeasor's ‹aiming' a tort at Texas. *Id.* at 211-2. ?Foreseeable injury alone is not sufficient to confer specific jurisdiction, absent the direction of specific acts toward the forum". *Id.* at 212. However, notes the court, ?when the actual content of communications with a forum gives rise to intentional tort causes of action, this alone constitutes purposeful availment". *Id.* at 213. In other words, when a German lawyer allegedly fraudulently induces a Texan to enter into a contract, that German has subjected himself to Texas jurisdiction.

A February, 2000 decision explained in further detail the important distinction between general jurisdiction and specific jurisdiction and how this distinction informs the *Calder v. Jones* effects test. *Alpine View Co. Ltd., et al. v. Atlas Copco AB, et al.*, 205 F.3d 208 (5th Cir. 2000). The *Alpine View* plaintiffs apparently used a stream-of-commerce argument to assert that subject matter jurisdiction was proper in Texas based on the *Calder v. Jones* test. *Alpine View* at 216. The problem with this argument, explains the court, is that since the *Alpine View* facts to not support a link between the contacts themselves and the litigation, this stream-of-commerce argument is intended to support general jurisdiction. *Id.* The Fifth Circuit, notes the court, has not allowed stream-of-commerce to support general jurisdiction. *Id.* More simply put, to make an ‹aimed tort' effects argument for personal jurisdiction, the contacts between the parties which would support specific jurisdiction must also give rise to the litigation itself; an argument that the same ‹aimed torts' would support general jurisdiction so that the court could decide another dispute between the parties would be a tough sell in the 5th Circuit.

Since *Calder v. Jones*, the Fifth Circuit has carved out a rule for applying an effects test to questions of specific jurisdiction. As the District Court in Dallas, citing *Wien Air*, recently noted: ?‹even a single act' directed toward a forum state that gives rise to a cause of action ‹can support a finding of minimum contacts.'" *The Bear Stearns Companies, Inc., et al. v. LaValle*, 2001 U.S.Dist. LEXIS 4913 (N.D. Tex. 2001), quoting *Wien Air*, at 211.

C. Which test should apply to domain name disputes?

At this point, there now exist two separate rules for personal jurisdiction in Texas which could apply to domain name disputes, the *Zippo* sliding scale and the *Calder v. Jones* effects test, as it has been clarified by the Fifth Circuit. Since the *Zippo* test, unlike the effects test, does not require any specific ‹aiming' by a defendant, it can be used to attempt to establish personal jurisdiction via a web presence in any case, regardless of the cause of action. The effects test, however, may well be a better bet when the web presence itself is at the root of the cause of action. My research did not turn up any 5th Circuit effects test decisions which directly confront this issue. The yet-unanswered question, then, becomes: is the registration of a trademark by a non-trademark owner ‹enough' to invoke subject matter jurisdiction under the effects test?

A pair of recent District Court decisions from Dallas and some dicta from the same court offer the beginning of an argument against the *Zippo* test in domain name cases. In both decisions, which involved claims that an out-of-state entity was infringing upon a Texas company's trademark via websites, the court held that *Zippo* did not allow for personal jurisdiction. *Fix My PC, L.L.C. v. N.F.N.*

Ass. Inc., 48 F.Supp. 2d 640 (N.D. Tex. 1999); *People Solutions, Inc. v. People Solutions, Inc.*, 2000 U.S. Dist. LEXIS 10444 (N.D. Tex. 2000). Significantly, the *Zippo* analysis did not inquire as to the nature and extent of the alleged wrong, but instead forced the court to look just to the interactivity of the infringing company's website. Factual questions such as the extent to which offending websites allowed Texas users to contract with the foreign companies informed the jurisdiction decision. In an effects test decision, however, the same District court implied that it would follow the 9th Circuit's lead and allow cybersquatting to provoke specific jurisdiction in the trademark holder's forum. *Bell Helicopter Textron, Inc. v. C&C Helicopter Sales, Inc., et al.*, 2001 U.S. Dist. LEXIS 3724, 13 (N.D. Tex. 2001). The Dallas Court refers to a famous 9th Circuit decision against a cybersquatter. *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

Yet another recent decision from this Dallas court comes closer to employing effects test analysis but instead ultimately uses the sliding scale to support specific jurisdiction. *American Eyewear, Inc. v. Peeper's Sunglasses and Accessories, Inc.*, 106 F.Supp.2d 895 (N.D. Tex. 2000). The *American Eyewear* defendant argued that the **?**operation of an Internet web site, without more, is insufficient to constitute conduct that is purposefully directed at Texas". *Id.*, at 900. In his opinion, Judge Fitzwater quickly notes that facts in the case suggest a *Zippo* middle ground between a passive website and internet contracting. *Id.*, at 901. Once in that middle ground, the Judge, as per *Zippo*, decides that the site in question is interactive enough to trigger specific jurisdiction. *Id.*, at 903. Towards the end of the opinion, thought, the Court adds a telling comment: **?**PI has attempted through its interactive web site to establish a retail presence in Texas. In doing so, it has purposefully availed itself of the privilege of conducting business here, and specific jurisdiction is proper." *Id.* While the court bases its decision that specific jurisdiction is proper on *Zippo* grounds, the language of the opinion suggests effects-type reasoning.

What does all this mean? It means that if a Texas client discovers that, say, a California company has taken his trademark and registered it as a domain name, there are a number of arguments which may support personal jurisdiction in Texas, and it is probably adviseable to assert more than one of them. First of all, depending on the nature of the offending website, *Zippo* may support general jurisdiction. Since, in a domain name case, the act of registration gives rise to the litigation, specific jurisdiction is possible. What's more, *Mink* seems to allow for a *Zippo* sliding scale to provide specific, as well as general, jurisdiction. Since only a single contact may sustain a finding of specific jurisidction, as opposed to the continuous contacts required of general jurisdiction, a *Zippo* specific jurisdiction test may not be too dificult. Certainly, if the offending web site allows for e-commerce, a good case can be made for specific jurisdiction under *Zippo*. (These were the facts of *American Eyewear*). What's more, the Dallas District court has suggested that specific jurisdiction would be proper under the effects test in a cybersquatting case. Therefore, a solid argument for specific jurisdiction via *Calder v. Jones* may be made even when the registrant/defendant has not even established a website, though there is no case law which directly supports this argument.

D. The problem of competitive registrations and jurisdiction

Finally, this leaves us with the question of a domain name registration by a competitor, or infringer, rather than by a cyber-squatter, where the offending web site is either clearly passive or does not even exist. Frankly, we have not found a Texas case where the effects test has been used to support jurisdiction in such a case, but we also have not found a Texas court which has said that trademark infringement is not sufficiently aimed conduct for *Calder v. Jones* jurisdiction. The *American Eyewear* case came closest, as the opinion's language argues towards effects-based jurisdiction, but Judge Fitzwater ultimately bases his decision on a sliding scale. for now, anyway, the answer may well be that the jurisdictional basis is difficult to

predict.

Many of the cybersquatting cases involve large companies, such as Ernest & Julio Gallo and Fisher Controls, which have the resources to simply sue the registrant where he lives. For a small business, however, domain name registration by a competitor presents a dificult situation: the high liklihood that the registrant will live somewhere other than Texas coupled with the inapplicability of the UDRP means that the jurisdictional decision will be critical. What's more, the internet itself allows for far greater damage to an out-of-state trademark than has previously been possible. Before the internet, a California lawyer doing business as Karl Bayer, Dispute Resolution Specialist may have had no real impact on my practice. Today, I spend substantial energy refining my web presence in the hopes that someday it will become a key tool for my practice, especially my ADR practice, by allowing me to communicate and share information with colleagues around the world. By the same token, though, a competitor, if he or she had karlbayer.com, would enjoy the same potential for havoc as I now enjoy for benefit. For the average small business, the prospect of waging a lawsuit in another state is a daunting one, but it is a more and more realistic scenario as more and more domain names are registered.

IV. THE NEW GENERIC TOP-LEVEL DOMAIN NAMES

We are currently in the midst of a fascinating new legal struggle about domain names. In November of 2000, ICANN decided to add seven new generic top-level domains (?gTLD"s) to the internet. *InterNIC FAQs on New Top-Level Domains*, <http://www.internic.net/faqs/new-tlds.html>, last visited 9/27/01. These are: .aero (for the air-transport industry), .biz (for businesses), .coop (for cooperatives), .info (for general use), .museum (for museums), .name (for individuals), and .pro (for lawyers, doctors, CPAs and the like). *Id.* While these new gTLDs will not require us to re-think the way we contend with domain name disputes, the manner in which domain names in these domains are distributed has been quite controversial. Essentially, we suddenly have the opportunity, all at once, to register domain names, like cheapusedcars, which have long been taken. What's more, trademark owners now must protect their marks all over again, since seven new avenues for infringement will soon exist. In order to try to protect trademarks, the new gTLDs will generally register domain names before they are launched, so that trademark holders will have some sort of priority, at least initially. The manner in which domain names for which more than one request is received has spawned the new dispute.

Speeches about the internet at CLE conferences such as this one have often described a future in which all case filing will be done at an ?online courthouse". A case will have its own secure website, and lawyers can upload and download documents as the case progresses. The introduction of new gTLDs has caused an interaction between technology and litigation which almost reaches this level. Neulevel.biz is the operator responsible for coordinating the launch of .biz. David Smiley, who has attempted to register the domains radio.biz and dj.biz, has sued ICANN and neulevel to enjoin the launch of .biz. Mr. Smiley argues that the process by which neulevel intends to process competing pre-launch domain name requests is an illegal lottery under California law. *Defendant Neulevel, Inc.'s Corrected Brief in Opposition to Plaintiffs' Motion for a Prelminary Injunction, Smiley, et al. v. ICANN, et al.*, Cause No. BC254659, in the Superior Case of the State of California, County of Los Angeles, filed September 26, 2001. Since .biz is the first of the new gTLDs to launch, the *Smiley* case will likely affect all the new gTLDs, so it is of great importance to the internet community. Therefore, all of the pleadings have been made available on the web, and commentary on each has quickly followed the filings. The ICANN watch website is an excellent portal to the ongoing litigation: icannwatch.org.

Since to delay this paper until the *Smiley* case has essentially decided how the new gTLDs may be registered would incur the further wrath of the State Bar, we will not offer extensive analysis of the

onging debate which may well have been proven wrong by the time of the speech. Instead, we will just note the existence of the new dispute and encourage readers to follow it s it develops. As the new domain names are registered, the process for protecting trademarks in them will be the same as for .com and the other original gTLDs. The dispute does, however, accent what is a driving force behind domain name disputes: the degree to which a .com domain name has become somethnig of a status symbol. A paper about the new gTLDs offers as a reason for their necessity ?the overcrowding of dot-com". *Journey to the Right of the Dot: ICANN's New Web Extensions*, VeriSign, Inc., <ftp://ftp.networksolutions.com/gtld/final_gtld_5_17.pdf>, last visited 9/28/02. Cybersquatting and domain name disputes are increasingly fueled by the importance of having a .com domain name, as .com was the original gTLD. This makes little sense, fundamentally, because the internet's significance comes from its ability to make information widely available quickly, even instantly. An ‹old' or ‹established' website should not be attractive, and yet the ‹old' domain names are the most valuable

V. CONCLUSION

Registering a domain name is remarkably easy. All you need is an internet connection, an available name, and roughly $40. This ease of acquisition, coupled with the fact that there can only be one of each name, has made domain names valuable commodities. Indeed, even as the World Trade Center buildings were falling, terrorist-attack related domain names were snatched up: americaattacked.com and sept112001.com reportedly were registered within twenty minutes of the attack. Harriet Ryan, *Giving name to tragedy: Domains are hot items in terrible times*, <http://dailynews.yahoo.com/h/ct/20010919/cr/giving_name_to_tragedy_domains_are_hot_items_in_terrible_times_1.html>, last visited 9/20/01. Cybersquatters are an easy example of what most people dislike about the internet, and they are fairly easy targets of the UDRP and the ACPA. However, what seems to be a potentially more damaging practice, the use of domain names to compete with trademark holders, remains relatively difficult to attack. Given the continuing uncertainy about personal jurisdiction in these cases, it may be a good bet for a competitive domain registrant that a trademark owner will see pursuit of the domain name as too expensive and too much hassle to be worthwhile.

Finally, at least in my own experience, while the cost of domain names is low, and the potential benefits of websites is high, the actual value of a domain name is tough to calculate. For example, there is no prominant Texas law firm to be found at the domain vinsonandelkins.com; instead, a web surfer is greeted with a site proclaiming the benefits of free speech, not unlike the SpinTopic site we saw earlier. Does the firm suffer for having to use the less convenient vinsonelkins.com? While maintaining a recognizable trademark as a domain name is increasingly important, it also seems important to maintain a sense of perspective and not register every name which may or may not reflect the trademark. If someone, for example, registers the domain name nflhotline.com, they can expect a threatening letter and maybe more from the National Football League, even though nfl.com and a host of other similar domains are safely in league hands. Ultimately, the soundest decisions seem to be the ones which acknowledge that while the internet may change the scope and focus of existing law, it does not require us to throw out what we know about subjects like personal jurisdiction in favor of completely new and internet-specific law.

APPENDIX A
15 U.S.C. §1125(d)(B)

(B)(i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to -

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;
(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
(VII) the person's provision of material or misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;
(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and
(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.

(B)(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.