The Anticybersquatting Consumer Protection Act's In Rem Provision: Making American Trademark Law the Law of the Internet?

Steven J. Coran
NOTE

THE ANTICYBERSQUATTING CONSUMER PROTECTION ACT’S IN REM PROVISION:
MAKING AMERICAN TRADEMARK LAW THE LAW OF THE INTERNET?

I. INTRODUCTION

Cybersquatting is a problem that has existed since mainstream use of the Internet became commonplace. Though there is no single definition of what cybersquatting is, most legal commentators tend to define the act of cybersquatting as the “deliberate, bad faith registration [of] domain names of well-known and other trademarks in the hope of being able to sell the domain names to the owners of those marks.”

Another similar act of cybertheft is called cyberpiracy. Cyberpiracy is defined as “the practice of registering domain names that incorporate variations on famous trademarks for the purpose of ‘taking unfair advantage of the reputation attached to those marks.’” The Anticybersquatting Consumer Protection Act (“ACPA”) expands the

2. See id. at 105. For purposes of this Note, the Author will refer to both the problems of cybersquatting and cyberpiracy as “cybersquatting.” The Anticybersquatting Consumer Protection Act (“ACPA”) uses the term “cyberpiracy.” See 15 U.S.C. § 1125(d) (Supp. V 2000).

[Cybersquatting is] an occurrence where a mark owner would like to establish a site on the Internet having the second level domain name consist mostly or entirely of the owner’s mark itself, but is unable to do so because someone has already registered that domain name, hoping that the mark owner will succumb to the “hold up” and enrich the domain name owner through a lucrative pay off.

Id. at 593; see also id. at 593 n.13 (footnote omitted) (noting that the “vast majority of commentators...confine cybersquatting to the ransoming scenario”).
definition to include also the "bad faith intent to profit" from a mark. A solution was needed for these newly recognized problems concerning the theft of intellectual property. Various methods of dealing with the problem of cybersquatting exist, ranging from the policies of Internet registries to international agreements. Because the Internet is global, in that virtually anyone with a computer can access any site, anywhere, the trademark laws of one nation should not become the "law" of the Internet, at least not without international agreement on that issue. This Note demonstrates that the ACPA, via its in rem provision, imposes American trademark law upon those living and using the Internet in other nations, and that other methods of combating cybersquatting should be used instead of the ACPA when those not under the personal jurisdiction of the United States courts are involved.

Part II of this Note gives an overview of Internet terminology and the problem of cybersquatting. Part III outlines several methods of domain name dispute resolution and describes the ACPA in detail. Part IV explains how the ACPA imposes American trademark law on non-Americans living outside of the United States and the problems associated with that. Part V concludes this Note with remarks about the deleterious global consequences of the ACPA's in rem provision.

II. INTERNET TERMINOLOGY AND THE PROBLEM OF CYBERSQUATTING

A. Basic Terminology of the Internet

Everyone today who uses computers probably has heard of the Internet. Even if one does not use a computer, he or she is probably still bombarded by advertisements for websites. These advertisements are placed in public transportation, billboards, magazines, newspapers, and virtually any other place where traditional advertisers advertise. Perhaps the epitome of the Internet becoming so mainstream is the fact that states advertise their websites. Pennsylvania, for example, displays its website on the bottom of the state’s new license plate, turning the residents into driving advertisements for their state and their state’s website.

4. See 15 U.S.C. § 1125(d)(1)(A)(i) (Supp. V 2000). The ACPA uses the title “Cyberpiracy prevention” in § 1125(d). Id. § 1125(d). When reading the statute as a whole, the ACPA combines the definitions of cybersquatter and cyberpirate into one, as opposed to the separate definitions legal scholars tend to give the terms. See supra notes 1-3 and accompanying text.

But what is the Internet? It is a giant network of computers. In fact, the Internet has been described as the “network of networks.” What this means is that a computer user can access data from anywhere across the world in the comfort of her own home or office. Accessing data is accomplished by logging one’s computer onto a website. Websites, their Uniform Resource Locator (“URL”) to be precise, contain domain names, which are “simply a computer[’s] address[es] in user-friendly form.” Having a domain name system (“DNS”) is quite user-friendly. Without it people would be forced to remember and enter a unique multi-digit string of numbers for every website they wish to log onto or for every e-mail recipient they wish to contact.

The DNS currently has two levels: top-level and second-level domains. Top-level domains (“TLDs”) include the generic TLDs (“gTLDs”) and country code TLDs (“ccTLDs”). The TLD is the last segment of the web address typed in when manually entering a web address. Several gTLDs exist, the most famous of which is .com. Other gTLDs include .net, .edu, .org, .gov, and .mil. If you have ever accessed websites in other countries, you probably have seen a ccTLD. These are two-letter country codes, such as .uk for the United Kingdom.

See id. Governor Ridge stated that “[l]icense plates are 72 square-inch billboards advertising our state,” and the purpose of placing the website on the plates was to “send a strong and positive signal to all who “see it—that Pennsylvania is high tech, high energy and ready for the new millennium.” Id.


8. See id. The multi-digit address is known as the Internet Protocol (“IP”) address, and is what the computer uses to pinpoint the location of a website. See id. For example, Hofstra University’s (www.hofstra.edu) IP address is 147.4.253.6. One can imagine how difficult it would be to have to remember a string of numbers for every website one wished to access, let alone having to e-mail someone by their IP address. The need for the domain name system (“DNS”) to simplify the process of accessing websites and sending e-mail seems obvious. To discover the IP address for a particular website, log onto http://www.webreference.com/cgi-bin/nslookup.cgi (last visited June 2, 2001).

9. See Lee, supra note 1, at 100.


11. See id.
and .ca for Canada. The consequences of having multiple TLDs will be explained later in this Note.

Second-level domains ("SLDs") are the letters that appear to the left of the TLD. SLDs commonly are words, names, brands, or trademarks which are "easy to remember and to identify without the need to resort to the underlying IP numeric address." Unfortunately, there is no version of the "yellow pages" to help find the location of a website, making a unique and on point SLD vital for people to find the websites they seek. A search engine can be helpful, but results can only be found based upon the keywords entered. As a consequence, a search engine will not always provide the results a person is seeking. Sometimes taking a guess at a domain name can reveal satisfying results, but that is not necessarily always the case. The problem is that there can only be one unique SLD for any TLD. One can only imagine the problems this could cause for people or companies trying to register domain names for their potential websites only to discover that the SLD they want has already been taken. With this in mind, the process of registering a domain name will be explained.

How is a domain name registered? From 1993 until the spring of 1999, the only way to register a domain name was through Network

---

12. As of this writing, there were at least 244 country code top-level domains ("ccTLDs"), ranging alphabetically from .ac (Ascension Island) to .zw (Zimbabwe). See A. Michael Froomkin, Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, 50 DUKE L.J. 17, 40 (2000). The ccTLDs derive from the International Organization for Standardization's ("ISO") Standard 3166. See id. at 40 n.63 (noting that "[the ISO, a private standards body, has created these codes for computer information systems processing purposes").

13. See infra Part II.B.

14. For example, in www.hofstra.edu, hofstra is the second-level domain ("SLD") and .edu is the top-level domain ("TLD").

15. Lee, supra note 1, at 101.

16. This should be familiar for those who have ever used LEXIS or WESTLAW. In addition, one must also register their websites with a particular search engine, so if the site is not registered, it will not show up on a particular search engine. Also, with the buyouts of search engines, the new owners would not want to allow a competitor of the owner to register and therefore advertise on the particular search engine.

17. See Jessica Litman, The DNS Wars: Trademarks and the Internet Domain Name System, 4 J. SMALL & EMERGING BUS. L. 149, 149-50 (2000); Baratta & Hanaman, supra note 7, at 334. For example, if one registered a website called www.stevencoran.com, no one else would be able to register the SLD "stevencoran" on the .com TLD. If they were so inclined to register a site under that name, they would have to use another TLD such as .org or .net. See Litman, supra, at 150.

18. See Litman, supra note 17, at 152-53 (discussing the problems encountered by businesses attempting to acquire domain names representing their trademarks only to find the marks were registered by others).

19. The Author decided on January 12, 2001 to register a domain name. The entire process took about five minutes. First, the Author went to www.nsi.com (Network Solutions) and at the opening screen, the website asked which site the Author wished to register. The Author entered
Solutions, Inc. ("NSI").20 The United States Department of Commerce granted NSI the exclusive right to register domain names.21 For six years, this Virginia-based American Company was the sole Internet domain name registry.22 An applicant would provide contact information, an application fee, and could choose an SLD name for whatever TLD was appropriate, usually .com for businesses and personal web pages.23 NSI at first distributed domain names on a first-come, first-served basis.24 In the early days of the Internet, one could have registered practically any word as the SLD, as long as the word was not already in use on any one particular TLD.25 NSI did not, and still does not, seriously scrutinize Domain name registry applications (though registrants are required to register in good faith), granting domain names even if they conflict with the rights not yet asserted by someone else.26

In 1998, with hopes of somewhat privatizing control of the Internet, the U.S. government chartered organizations that later merged into the Internet Corporation for Assigned Names and Numbers ("ICANN").27

See Baratta & Hanaman, supra note 7, at 345 (describing Network Solutions, Inc. ("NSI") as a "quasi-governmental entity ... [and] the sole agency responsible for the registration of domain names").


As a result, all in rem trademark litigation against a domain name would only have been possible in the Eastern District of Virginia, where Network Solutions is located in the federal court system. See Lee, supra note 1, at 127-32.

See id. at 102-03; Litman, supra note 17, at 151. Not all gTLDs are appropriate for particular websites. Certain gTLDs are open (.com, .net, .org) and any person or entity can register names within them, as long as the SLD is not already taken for that particular gTLD. Other gTLDs are restricted (.int, .edu, .gov, and .mil) and are available only to international, educational, governmental, and military entities. See Lee, supra note 1, at 100.

See Lee, supra note 1, at 102; Litman, supra note 17, at 151; Tysver, Domain Name Disputes, supra note 10. The policy was later changed several times and was still obviously considered inadequate by Congress, as it passed the ACPA in 1999.

See Litman, supra note 17, at 150-51.

See Lee, supra note 1, at 102-03; Baratta & Hanaman, supra note 7, at 345.

ICANN is "the primary entity through which Internet policy is established." Though ICANN was created as a result of American governmental action, it is administered by a board of nineteen international directors and various supporting organizations. The supporting organizations of ICANN were designed to "help . . . promote the development of Internet policy and encourage diverse and international participation in the technical management of the Internet." 

In April 1999, ICANN announced that other entities besides NSI could act as domain registries, ending NSI's monopoly of the distribution of domain names. Just like other industries on the web, the domain registry industry grew very quickly. As of December 11, 2001, there were eighty-nine accredited and operational domain name registries world-wide. Forty-six of these registries are located in the United States. In addition, all registries of the .com, .net, and .org TLDs, as well as a small number of ccTLDs, must be accredited by ICANN, and thus must follow ICANN's policies. Besides ICANN, the World Intellectual Property Organization ("WIPO"), a specialized agency of the United Nations, is also involved with the governance of the Internet. WIPO specifically administers international intellectual property treaties and helps to protect intellectual property world-wide.

28. Baratta & Hanaman, supra note 7, at 340 (explaining that ICANN privately governs IP address space allocation, domain name system management, and root server system management functions).
30. ICANN, Supporting Organizations, at http://www.icann.org/general/support-orgs.html (last modified Feb. 2, 2000); see also Baratta & Hanaman, supra note 7, at 340-43 (defining and discussing the functions of the ICANN Supporting Organizations).
32. See ICANN, List of Accredited and Accreditation-Qualified Registrars, at http://www.icann.org/registrars/accredited-list.html (last modified Dec. 11, 2001). There are also seventy-two accredited, but not yet operational, registrars in the .com, .net, and .org TLDs, thirty-seven of which are located in the United States. See id.
33. See id.
34. See Baratta & Hanaman, supra note 7, at 344; see also ICANN, Uniform Domain Name Dispute Resolution Policy (Oct. 24, 1999), at http://www.icann.org/udrp-policy-24oct99.htm (last modified Jan. 3, 2000) [hereinafter ICANN, Dispute Resolution Policy]. The .com, .net, .org, and .int registries and domain name owners are contractually obligated to use the UDRP, formulated by ICANN and the World Intellectual Property Organization ("WIPO"), when a dispute arises (though complainants can also resort to the court system). See WIPO, WIPO to Probe New Issues Relating to Domain Name Abuse, at http://wipo2.wipo.int/process2/press/235.html (last visited Oct. 2, 2000) [hereinafter WIPO, Domain Name Abuse].
35. See WIPO, Domain Name Abuse, supra note 34.
36. See Baratta & Hanaman, supra note 7, at 344.
Both of these organizations have helped to create a domain name dispute resolution policy that is discussed later in this Note.  

B. The Problem of Cybersquatting

As stated above, there can only be one unique SLD per TLD. Thus, a domain name is a unique and valuable resource. As a consequence, no matter how upset a potential domain name registrant might become about it, the fact is that there can only be one www.basketweaving.com. This creates the possibility of conflict over the precious resource that is a domain name. After overcoming the anguish of not being able to register www.basketweaving.com because the name is already taken, the enterprising basketweaver will have to come up with an alternative name for the website. One of the largest problems in domain name disputes is the problem of cybersquatting. Cybersquatting is the practice of registering, in bad faith, an SLD that incorporates someone else’s service or trademark, usually with the intent of extorting money from the mark holder in a resale of the domain name to the mark holder. Because there are multiple TLDs, it is possible for a mark holder’s mark to be used as a cybersquatter’s SLD on more than one TLD. So even though the mark holder might win a battle with a cybersquatter on one TLD, that same mark holder might have to fight that same cybersquatter again on a different TLD. The more TLDs there are, the greater the opportunity for cybersquatting.

To provide an example of cybersquatting, imagine that the year is 2040, and an up-and-coming toy manufacturer finally creates a stuffed animal that it believes would sell not only to children but to adults as well. The toy is named “Babyguin,” and is a plush Emperor penguin chick. Everyone who sees a Babyguin immediately falls in love with it. Prior to putting Babyguin on the market, the manufacturer obtains a trademark for the item. John Doe, who is fifty years old, hears from an

37. See infra notes 62-75 and accompanying text.
38. See supra note 17 and accompanying text.
39. See Litman, supra note 17, at 153 (discussing the dilemma faced by companies whose trademarks are being used as domain names by prior registrants); Baratta & Hanaman, supra note 7, at 334.
40. See Litman, supra note 17, at 153; Baratta & Hanaman, supra note 7, at 334.
41. See Baratta & Hanaman, supra note 7, at 334-35. The Author suggests either www.APbasketweaving.com (for the high school intellectual basketweaver) or www.korbweber.com (for the German basketweaver).
42. See Lee, supra note 1, at 104-07.
unknown source that Babyguin is about to be placed on the market. Mr. Doe, remembering the Beanie Baby craze from his youth, realizes that a lot of money could be made from the Babyguin product. Immediately, Mr. Doe registers www.babyguin.com with a domain registry, spending seventy dollars for the registration fee. Both the manufacturer and Mr. Doe are correct in their predictions. Babyguin becomes the best selling toy in the United States practically overnight. The manufacturer, quite logically, wants to increase his sales by selling Babyguin on the Internet so that the entire population of the United States can buy the product from their homes. Unfortunately, when the manufacturer tries to register www.babyguin.com, it discovers that the domain name is already taken.

The CEO decides to log onto the current www.babyguin.com and he is disturbed to read the following message that appears in plain text across the screen:

"Dear Manufacturer of Babyguin: Shall we begin the bidding for the sale of this website? I’ve always wanted a house off River Road in Potomac, Maryland and a Porsche 911 Turbo. Please call me at (555-555-5555)."

The preceding hypothetical was a slightly exaggerated example of something that happens not too infrequently when it comes to cybersquatting cases. The situation sometimes becomes more difficult when the mark holder is unable to discover the true identity of the cybersquatter because the cybersquatter registered the domain name using a pseudonym. Other problems arise when the cybersquatter lives outside of the United States. In that situation, the cybersquatter is not subject to in personam jurisdiction unless the cybersquatter in some way

44. See S. Rep. No. 106-140, at 7 (1999) ("Instances of cybersquatting continue to grow each year because there is no clear deterrent and little incentive for cybersquatters to discontinue their abusive practices."). The king of early cybersquatters was Dennis Toeppen. Toeppen registered over 100 domain names (all famous ones, such as panavision.com and deltairlines.com) with the intent of selling the domain names to the trademark holders. When Panavision’s counsel approached Toeppen telling him to stop using the domain name, Toeppen then responded directly to Panavision with the classic cybersquatter’s demand:

If your attorney has advised you otherwise, he is trying to screw you. He wants to blaze new trails in the legal frontier at your expense. Why do you want to fund your attorney’s purchase of a new boat... when you can facilitate the acquisition of “PanaVision.com” cheaply and simply instead?

Panavision Int’l, L.P. v. Toeppen, 141 F.3d 1316, 1319 (9th Cir. 1998). Toeppen demanded $13,000 from Panavision in exchange for transferring the domain name to them. See id.

45. See Lee, supra note 1, at 106.
Why is there a need for marks? It has been said that “[t]he purpose of trademark law is to promote economic efficiency and incentivize businesses to invest in a mark, to the benefit of the consumer.” 53 Trademarks benefit consumers by relieving them of the task of determining the quality of goods and services at every time of purchase. 54 For example, rather than physically inspecting each and every pair of jeans to determine their quality, the consumer can just rely on the mark name of Levi’s. If it turns out that the jeans are of low quality, the consumer will no longer purchase that particular brand. This provides incentive for the producer to make a quality product, and the mark makes it easier for the consumer to shop and spend money, which helps stimulate the economy. 55 In time, the mark can become so famous that consumers begin to incorporate trademarks into their common parlance. 56 Those of us who blow our noses with Kleenex or wore Pampers as infants, yet did not actually use the Kleenex or Pampers brands, are guilty of this.

The use of marks is particularly relevant to the Internet because people tend to have no idea how to find a website besides taking a guess at the site’s URL. 57 People will usually guess the common name of something they are looking for, which sometimes just happens to be the service’s or product’s mark. Cybersquatting therefore poses a problem to the mark holder because the domain name that would be best for business, the one that the product or service is most commonly known by, is not available. 58

What can a mark holder do upon discovering that the domain name that corresponds to his or her mark is unavailable? 59 If the domain name


54. See id.

55. See id. at 1834.

56. In its extreme form, the incorporation of marks into common parlance is exemplified in the southern United States. There, the term “Coke” means not just the particular brand of carbonated beverage that is known the world over, but it actually refers to all carbonated beverages, including even Pepsi. In short, Coke means to Southerners what “soda” or “pop” means to the rest of the English-speaking world. See generally Mark Zaloudek, The Catch-22 of Brand Names, SARASOTA HERALD-TRIB., Aug. 27, 2001, at B1 (describing how brand names are commonly used to refer to a product generally rather than the brand name specifically).

57. See Lee, supra note 1, at 101; Baratta & Hanaman, supra note 7, at 335-36.

58. See Baratta & Hanaman, supra note 7, at 335-36.

59. It is important to remember that not all domain name disputes involve cybersquatters. This is true even if the domain name holder happens to register as his domain name the trademark of someone else. The key to classifying someone as a cybersquatter is the bad faith requirement.
has the constitutionally required minimum contacts with the forum.\footnote{46} The possibilities and problems of allowing in rem jurisdiction over the domain name itself will be discussed in great detail later in this Note.\footnote{47} The problems created by the first-come, first-served nature of domain registries need to be resolved. The next section of this Note outlines the various methods used to resolve domain name disputes.

### III. METHODS OF DOMAIN NAME DISPUTE RESOLUTION

Before beginning the discussion of domain name dispute resolution procedures, a cursory review of mark law is in order. Trademarks are symbols, phrases, and words that are used to identify a particular person’s products and distinguish those products from the products of another person.\footnote{48} However, the service mark is even more relevant to the problem of cybersquatting. Service marks are also symbols, phrases, and words, but they are used to identify a particular person’s services and distinguish those services from the services of another.\footnote{49} For the sake of simplicity, this Note treats both of these terms the same and refers to both as marks.\footnote{50} The protection of marks is governed by both state and federal law.\footnote{51} However, federal law has dominated the law of marks since the late nineteenth century, and especially since the passage of the Lanham Act in 1946.\footnote{52}

\footnote{46} In \textit{International Shoe Co. v. Washington}, 326 U.S. 310 (1945), the United States Supreme Court held:

\begin{quote}
[D]ue process requires only that in order to subject a defendant to a judgment \textit{in personam}, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice."
\end{quote}

\textit{Id.} at 316 (citations omitted).

\footnote{47} See discussion \textit{infra} Part III.

\footnote{48} See 15 U.S.C. § 1127 (1994). An example of a trademark would be the name Coca-Cola or Levi’s. Those names are words that help identify the producer’s products and help distinguish them from Pepsi-Cola and Lee, respectively.

\footnote{49} See \textit{id.} An example of a service mark would be Verizon (formerly Bell Atlantic) or the Potomac Electrical Power Company (PepCo). Rather than sell a product, these companies provide services, phone and electricity, respectively. But like a product, there is also the need to identify and distinguish one’s service from the services provided by others. See \textit{id.} The definitions of certification marks and collective marks are not necessary for the purposes of this Note.

\footnote{50} See \textit{id.} (defining "mark" as including trade, service, collective, and certification marks).


\footnote{52} Lanham Act, 15 U.S.C. §§ 1051-1127 (1994 & Supp. V 2000). Congress stated that the intent of the Lanham Act "is to regulate commerce within the control of Congress." \textit{Id.} § 1127. Because this Note focuses solely on federal mark law, it is beyond its scope to further discuss state common law marks.
holder demands money, then the mark owner, depending on his or her wealth, could pay the price. However, “for some paying a cybersquatter for a domain name [feels] a lot like making a deal with Darth Vader. Although they lived to fight another day, these persons would prefer to avoid the experience altogether.”

A. The Uniform Domain Name Dispute Resolution Policy

Before considering the solutions that involve litigation, this Note discusses the policy that every domain registrar for .com, .org, .net, and .int and domain name owner contract to use in the event of a dispute.

In October of 1999, ICANN approved the Uniform Domain Name Dispute Resolution Policy (“UDRP”) for mandatory use in all domain name disputes. The UDRP is required to be used by all persons or entities who register domain names with an ICANN-accredited domain registry. These persons or entities are contractually obligated to submit
to an administrative proceeding with an ICANN-approved dispute-resolution service:

In the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and (ii) you have no rights or legitimate interests in respect of the domain name; and (iii) your domain name has been registered and is being used in bad faith.

If the mark owner successfully proves these three elements in the mandatory proceeding, the remedy is that the domain name may either be canceled or transferred to the mark owner. The use of these mandatory arbitration proceedings does not preclude either party from litigating the dispute in the court system, either before the mandatory proceeding begins or after it ends. Unlike in litigation, especially that involving the ACPA, there are no monetary awards available under the UDRP. This, however, is offset by the reduction in costs by using arbitration rather than litigation. The costs of these procedures are much less than the costs of a litigation-based alternative which can be an

---

(a) the statements that [registrant makes] in [registrant's] Registration Agreement are complete and accurate; (b) to [registrant's] knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) [registrant is] not registering the domain name for an unlawful purpose; and (d) [registrant] will not knowingly use the domain name in violation of any applicable laws or regulations. It is [registrant's] responsibility to determine whether [registrant's] domain name registration infringes or violates someone else's rights.

Id. ¶ 2.

65. However, one is not enjoined from initiating litigation before the mandatory proceeding or after the mandatory proceeding has ended. See id. ¶ 4(k).

66. See ICANN, Approved Providers for Uniform Domain Name Dispute Resolution Policy, at http://www.icann.org/udrp/approved-providers.htm (last updated May 21, 2000) (including a list of the currently four available services, including WIPO's Arbitration and Mediation Center which is located in Switzerland and was the first approved provider).

67. ICANN, Dispute Resolution Policy, supra note 34, ¶ 4(a).

68. See id. ¶ 4(i); see also Tysver, Domain Name Disputes, supra note 10.

69. See ICANN, Dispute Resolution Policy, supra note 34, ¶ 4(k). For a misapplication of this provision, see infra note 130.

70. See id. ¶ 4(i).

71. See WIPO, Schedules of Fees under the ICANN Policy (effective Aug. 15, 2000), at http://arbiter.wipo.int/domains/fees/index.html (last visited June 2, 2001). If one through five domain names are in dispute between two parties, the cost of a single panelist to make the UDRP-mandated decision is $1500. This cost is to be borne by the complainant. However, if the domain name holder wishes to have a three member panel making the decision, then the cost doubles to $3000 and the costs are split between the two parties. See ICANN, Dispute Resolution Policy, supra note 34, ¶ 4(g).
expansively greater amount of money. In addition, the UDRP also sets out various standards for proving bad faith in defending a person's, or entity's, interest in the domain name, which in practice is not as biased in favor of the mark holder as the ACPA's provisions tend to be.\(^7\)

The first UDRP proceeding was concluded on January 14, 2000.\(^7\)

The WIPO Arbitration and Mediation Center panel ruled that possession of the website www.worldwrestlingfederation.com should be transferred from the possession of a California resident to the mark holder, World Wrestling Federation Entertainment, Inc.\(^7\) It is important to re-emphasize that because most major domain name registries are required to be accredited by ICANN (and therefore must follow the UDRP), everyone who registers a domain name on a gTLD, no matter where the hopeful future domain name owner resides, is subject to the "jurisdiction" of the UDRP.\(^7\)

72. ICANN enumerates the following examples of bad faith use of domain name: (1) "acquiring the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name" to the mark holder for more than the seller's (domain name owner's) "out-of-pocket costs" for registering the domain name; (2) registering the domain name to prevent the mark holder from using the mark in a corresponding domain name; (3) registering the domain name mainly for "disrupting the business of a competitor"; or (4) using the domain name in a way that intentionally attracts, for commercial gain, the attention of Internet users by confusing them into believing domain name holder's website is being endorsed by the mark holder. ICANN, Dispute Resolution Policy, supra note 34, \S 4(b).

Unique to the UDRP is its list of factors showing what constitutes legitimate use of a domain name that corresponds to another entity's mark. See id. \S 4(c). Bias in the ACPA will be discussed infra Part III.C.


74. See World Wrestling Fed'n Entm't, Inc. v. Bosman, No. D-99-0001 (Admin. Panel Jan. 14, 2000), available at http://arbiter.wipo.int/domains/decisions/html/d99-0001.html (last visited Sept. 29, 2000). The panel found that Bosman's use of the domain name was in bad faith because he had no legitimate interests with respect to the domain name. See id. \S 2. It is important to note that Bosman registered the domain name with MelbourneIT, an Australian registrar. The ACPA would not permit in rem jurisdiction in this case, but if the opposite had happened, and an Australian registered a website from an American registrar, there would be in rem jurisdiction. By not using the ACPA, international consequences are avoided. See infra Part IV.

75. See ICANN, Dispute Resolution Policy, supra note 34, \S 1 & n.2. This is important because the ACPA allows for in rem jurisdiction over the domain name, and as a result arguably would impose American trademark laws over those not present in the United States. The UDRP is at least somewhat international in character, and all trademarks from every country are treated equally.
B. Mark Infringement and Dilution Causes of Action

Prior to the passage of the ACPA, the only litigation-based solutions were to file a mark infringement or mark dilution action. Mark infringement occurs when the mark of one party is used by another party in a manner that is likely to cause consumer confusion as to the source of the goods or services. Mark dilution exists only when a famous mark is "blurred" or "tarnished." Blurring occurs when the strength of the mark is weakened by its identification with dissimilar goods. The tarnishing of a mark is distinguished from the blurring of a mark because, in the tarnishing situation, the mark is placed in an unflattering light. This is usually done by associating the mark with an inferior or obscene product or service.

76. See Federal Trademark Dilution Act, 15 U.S.C. § 1125(c) (Supp. V 2000) (forbidding the use of another's trademark when the use could cause confusion among potential customers); see also Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1324 (9th Cir. 1998) (applying the Federal Trademark Dilution Act to a cybersquatting case and ordering the transfer of the domain name from the cybersquatter to the plaintiff). But see Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 874 (9th Cir. 1999) (limiting application of the Federal Trademark Dilution Act to prevent overprotection of trademark holders' rights).

77. See Polaroid Corp. v. Polarad Elec. Corp., 287 F.2d 492, 495 (2d Cir. 1961). In order to determine consumers' likelihood of confusion, the courts will examine several factors, including: (1) the strength of the mark; (2) the proximity of the goods; (3) the similarity of the marks; (4) evidence of actual confusion; (5) the likelihood that the prior owner will bridge the gap; (6) the defendant's good faith in adopting the mark; (7) the quality of the defendant's product; and (8) the sophistication of the buyer. See id.

78. Section 1125(c)(1) states that marks may be considered "famous" based on consideration of the following factors:

(A) the degree of inherent or acquired distinctiveness of the mark;
(B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;
(C) the duration and extent of advertising and publicity of the mark;
(D) the geographical extent of the trading area in which the mark is used;
(E) the channels of trade for the goods or services with which the mark is used;
(F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;
(G) the nature and extent of use of the same or similar marks by third parties; and
(H) whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.


79. See Berkman Center for Internet & Society at Harvard Law School, Overview of Trademark Law, at http://cyber.law.harvard.edu/setschool/fishd/field/domain/tm.htm (last visited June 2, 2001) (providing Kodak-brand bicycles or Xerox-brand cigarettes as examples of mark blurring).

80. See id.

81. See Toys "R" Us, Inc. v. Akkaoui, No. C-96-3381-CW, 1996 U.S. Dist. LEXIS 17090, at *7 (N.D. Cal. Oct. 29, 1996) (holding that defendant's "Adults R Us" domain name "tarnishes the 'R Us' family of marks by associating them with a line of sexual products that are inconsistent with the image 'Toys 'R' Us' has striven to maintain for itself").
In practice, the application of traditional trademark law to domain name disputes is limited, with accordingly restricted results.\(^{82}\) One reason for the limited application of traditional trademark laws to domain name disputes is that these causes of action require commercial activity by the defendant as an element of a violation.\(^{83}\) The act of registering a domain name that corresponds to someone else’s mark and doing nothing further would not qualify as commercial activity, and thus, there would be no remedy under traditional trademark law.\(^{84}\) Besides limited results and applicability,\(^{85}\) litigation is also much more expensive than utilizing the UDRP.

C. The Anticybersquatting Consumer Protection Act

As an attempt to circumvent the inadequacies of traditional trademark law,\(^{86}\) another litigation-based alternative was created in the recently passed ACPA.\(^{87}\) The ACPA states:

A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—

(i) has a bad faith intent to profit from that mark, including a personal name . . . and

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

---

83. See Cheatham, supra note 60, at 52.
84. See id. at 52-53 nn.74-79; infra notes 86-90 and accompanying text.
85. In fact, courts had determined that prior to the ACPA, federal trademark dilution actions did not allow for in rem jurisdiction over the offending website. See Porsche Cars N. Am., Inc. v. Porsch.com, 51 F. Supp. 2d 707, 711 (E.D. Va. 1999), vacated sub. nom. Porsche Cars N. Am., Inc. v. Allporsche.com, 215 F.3d 1320 (4th Cir. 2000). The district court decision was vacated by the Fourth Circuit because the ACPA, which permits in rem jurisdiction, allows retroactive application of its use, and the ACPA was enacted after the district court case. Also, it is important to note that mark dilution can only be used if the mark is “famous.” The UDRP and the ACPA are not so limited.
86. See Bensusan Rest. Corp. v. King, 126 F.3d 25, 27 (2d Cir. 1997) (stating that the court “realize[s] that attempting to apply established trademark law in the fast-developing world of the [Internet is somewhat like trying to board a moving bus”).
(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark.\(^8\)

A key difference between the ACPA and traditional trademark law is that in the ACPA, there is no requirement that the domain name owner use the website in connection with goods and services.\(^9\) The ACPA, unlike a mark dilution cause of action, does not require "commercial use" of the mark by the domain name owner in order for the mark holder to have a cause of action.\(^10\)

In determining the bad faith of the person who registers a mark as a domain name, the ACPA gives a suggested list of factors to consider.\(^11\)

\(^8\) Id. § 1125(d)(1)(A).
\(^9\) Compare the ACPA, id. § 1125(d)(1)(A) (stating that "[a] person shall be liable in a civil action by the owner of a mark . . . if, without regard to the goods or services of the parties"), with Lanham Act, 15 U.S.C. § 1125(a)(1) (1994) (requiring "connection with any goods or services").
\(^11\) The ACPA states that a court may consider, but is not limited to, factors such as the following:

(I) the trademark or other intellectual property rights of the person [referring to the alleged cybersquatter], 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 and 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 [15 U.S.C. § 1125(c)(1)].

When personal jurisdiction is invoked, the ACPA also allows, in addition to transfer of the domain name, the award of actual and statutory damages ranging from $1,000 to $100,000 per domain name. This alone could be used by mark holders to intimidate those who in good faith use marks as their SLD into relinquishing the domain name. This comes despite the fact that the statute states that "[b]ad faith intent ... 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." Unsophisticated computer users will probably not be aware of the aforementioned provision, and thus would readily relinquish their domain name after the thought of a potential $100,000 fine entered the equation. This produces the possibility of abuse, which will be discussed later in this Note.

Unique to the ACPA, and what this Note draws contention with, is the provision for in rem jurisdiction under the act. In rem jurisdiction can be useful to a mark holder who cannot identify the registrant of a website or when that registrant is not within the personal jurisdiction of the court, which would apply mostly to those who do not reside within the United States. In those situations, the ACPA allows the owner of the mark to file suit against the domain name itself in the judicial district where the domain registry is located. By allowing this, Congress has in essence decided that a domain name is a res. The courts tend to find

93. Not all use of an entity's mark as a domain name is use in bad faith. Although the ACPA and the UDRP are often used to the advantage of corporations, there are some situations where, at least in theory, such a use will not constitute bad faith. An example of a good faith registration that a mark holder would still seek to quash with the ACPA would be if someone with the last name Lockheed decided to register the domain name for the purposes of posting pictures of his or her immediate family. The aviation giant, of course, would want that domain name, but without being able to satisfy the elements of bad faith required by the ACPA, it should not be able to obtain it. The ACPA also states that "[b]ad faith intent ... 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." Id. § 1125(d)(1)(B)(ii).
94. This practice of intimidating domain name owners into relinquishing their domain names upon the threat of legal action and up to $100,000 in fines is called reverse domain name hijacking. See Mark Grossman & Allison K. Hift, Is the Cybersquatting Cure Worse Than the Disease?, LEGAL TIMES, Jan. 24, 2000, at 24. Recently, the owners of Gumby and Pokey threatened a twelve year old who had registered the domain name Pokey, which was the child's nickname. See id.
96. See infra notes 103-08 and accompanying text.
97. See Lee, supra note 1, at 106, 124-25.
99. Although the Author would like to discuss this issue in more depth, it is worthy of a Note topic on its own.
bad faith in cybersquatting cases under the ACPA rather easily, especially when any form of financial compensation is considered in exchange for the domain name.\textsuperscript{100} Also, the courts will hold against the domain name owner the fact that he or she has previously registered multiple sites that are confusingly similar with another's mark,\textsuperscript{101} even though the particular domain name at issue in the litigation may only be on the border of constituting bad faith. The fact that the domain name owner has done these sorts of things in the past will tip the scale against him or her.\textsuperscript{102}

These factors have led some legal scholars, such as Professor A. Michael Froomkin, to fear "that the legislation may end up reducing the visibility of online political activism, by making it difficult for protesters to latch onto a company name to launch a critical Website."\textsuperscript{103} Also, Senator Patrick Leahy voiced First Amendment concerns about the ACPA, particularly with regard to its potentially restrictive effect on online criticism.\textsuperscript{104} An example of this was the recent attempt by Verizon

\textsuperscript{100} Because the ACPA states that "the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner . . . 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," 15 U.S.C. § 1125(d)(1)(B)(i)(VI), any attempt by the domain name owner to even consider financial compensation for the return of the domain name, can be used as evidence of bad faith. For example, in Broadbridge Media LLC v. Hypercd.com, 106 F. Supp. 2d 505 (S.D.N.Y. 2000), the district court primarily based its finding of domain name holder bad faith on the holder's repeated offers to sell the domain name. See id. at 512. The court did not consider the fact that the mark holder was negligent in failing to renew the hypercd.com SLD, nor did the court consider that the mark holder began negotiations for an exchange of money for the domain name. See id. Apparently, if the domain name holder even considers a monetary offer or appears interested, bad faith can be found.

\textsuperscript{101} See 15 U.S.C. § 1125(d)(1)(B)(i)(VII). A history of this practice may be considered evidence of bad faith:

[T]he 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.

\textit{Id.; see also} N. Light Tech., Inc. v. N. Lights Club, 236 F.3d 57, 65 (1st Cir.) (stating that "the defendants' numerous registrations of domain names containing the trademarks of others . . . represented powerful evidence of defendants' bad faith in operating" the site at issue in the case, northernlights.com), cert. denied, 121 S. Ct. 2263 (2001).

\textsuperscript{102} See N. Light Tech., Inc., 236 F.3d at 65.


\textsuperscript{104} See Cybersquatting and Consumer Protection: Ensuring Domain Name Integrity: Hearing on S. 1255 Before the Senate Comm. on the Judiciary, 106th Cong. 41-44 (1999) (statement of Sen. Patrick Leahy). At the committee hearing on the ACPA, Senator Leahy stated:

The bill would criminalize dissent and protest sites. A number of Web sites collect complaints about trademarked products or services, and use the trademarked names to identify themselves. For example, there are protest sites named "boycott-cbs.com" and
Communications to quell critical online sites. Verizon, the former Bell Atlantic and GTE, decided to register fifty-seven self-critical domain names,\textsuperscript{105} including www.verizonsucks.com, perhaps with the hope of preventing the registration of all websites critical of Verizon. 2600, a hacker magazine, later registered www.verizonreallysucks.com, causing Verizon to send a cease and desist letter to the organization stating that they had violated the ACPA and demanding that the organization cease all use of the website.\textsuperscript{106} Verizon never actually filed suit against 2600, probably from publicity over the issue.\textsuperscript{107} Of more concern to the free speech advocate would be the successful application of the ACPA by People for the Ethical Treatment of Animals ("PETA") against the domain name owner of www.peta.org.\textsuperscript{108} But in short, taking away someone's website via the ACPA is not that difficult a task, First Amendment challenges aside. Regardless of the possible violation of First Amendment rights, the ACPA has been a success in effectively confronting the problem of cybersquatting via both its arms: \textit{in personam} and \textit{in rem} jurisdiction.\textsuperscript{19}

\textsuperscript{19}"www.PepsiBloodbath.com." While the speech contained on those sites is clearly constitutionally protected, [the ACPA] would criminalize the use of the trademarked name to reach the site and make them difficult to search for and find online. \textit{Id.} at 44 (emphasis added).


\textsuperscript{107} See \textit{id}. Verizon claims that they realized that 2600's use of the Verizon mark was a fair use, and they further claimed that they are "out to defend [their] brand against confusion and dilution, not squelch free speech." Streitfeld, \textit{supra} note 105.

\textsuperscript{108} See \textit{People for the Ethical Treatment of Animals, Inc. v. Doughney}, 113 F. Supp. 2d 915, 920 (E.D. Va. 2000). Defendant Doughney registered www.peta.org as "People Eating Tasty Animals" and People for the Ethical Treatment of Animals ("PETA") sought to use the ACPA to shut down Doughney's site. The court rejected Doughney's "parody" defense, by stating: "A parody exists when two antithetical ideas appear at the same time," \textit{id.} at 921, and because PETA did not have a website at the time, the two sites could not have simultaneously existed, and a parody could thus not exist. \textit{See id.} at 921. According to the court's logic, no critical site or parody may exist that involves using the mark of another in the domain name, unless the mark holder has a website. \textit{See id.} at 920. The court also disregarded Doughney's First Amendment defense, stating that PETA only wanted Doughney to stop using their mark, and was not trying to stop criticism of PETA. \textit{See id.} at 921. According to this logic, Verizon would prevail in a case against the domain name owner of www.verizonreallysucks.com.
IV. THE ACPA AND THE IMPOSITION OF AMERICAN TRADEMARK LAW UPON THE ENTIRE WORLD

The use of the ACPA in in rem cases where the domain name owner does not reside in the United States is not consistent with the comity of nations. By applying the ACPA to those who do not reside in the United States, Congress is in essence making U.S. mark law the mark law of the global Internet. This is something that should not be allowed to stand, given the international and borderless realities of the Internet.

A. The Internet is a Global and Not a Uniquely American Medium

In July 1997, the White House revealed the government’s intention of privatizing control of the Internet’s domain name system with the release of A Framework for Global Electronic Commerce. The framework set out various principles that should guide the development of the Internet. Among these principles were that:

(1) The private sector should lead; (2) Governments should avoid undue restrictions on electronic commerce; (3) Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce; (4) Governments should recognize the unique qualities of the Internet; [and] (5) Electronic commerce over the Internet should be facilitated on a global basis.

In 1998, the Department of Commerce released two proposals for privatization of the DNS, the Green Paper and the White Paper. The White Paper was the result of various commentaries by the public concerning the Green Paper and the responses provided by the government regarding those comments. In particular, some comments about the Green Paper expressed concern that it did not adequately

110. Id. at 513-14.
113. See id. at 31748.
provide for globalization of the DNS.\footnote{See id.} In response to this concern, the White Paper stated:

The U.S. Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management.\footnote{Id.}

These ideas somewhat came into fruition with the creation of ICANN, as stated earlier.\footnote{For an article criticizing ICANN as an unconstitutional delegation of government powers by the Department of Commerce, see Froomkin, \textit{supra} note 12.} Regarding the issue of cybersquatting, the White Paper recommended that domain name registrants should “submit to and be bound by alternative dispute resolution systems identified by [the proposed organization to handle these matters, which later became ICANN] for the purpose of resolving those conflicts.”\footnote{White Paper, \textit{supra} note 112, at 31750.} Clearly, the Clinton administration intended for domain name disputes to be settled on an supranational basis.\footnote{The Clinton Administration initially opposed the ACPA bill, stating that the bill “takes a unilateral U.S. approach that interferes with efforts to develop a worldwide process to resolve domain-name disputes.” Carolyn Lochhead, \textit{Web-Address Legislation Called Flawed: Corporations Could Dominate Small Firm Sites, Experts Say}, S.F. CHRON., Nov. 18, 1999, at A1. Lawmakers attached the ACPA measure to a satellite bill that President Clinton was eager to sign in order to prevent him from vetoing it. \textit{See id.}} However, with the passage of the ACPA, it appears that, when \textit{in rem} jurisdiction is invoked, American mark law seems to have become the law of the Internet.

\textbf{B. The Effect of the In Rem ACPA Cases}

To date, there have only been a few court decisions regarding \textit{in rem} jurisdiction and the ACPA.\footnote{The Author intends to briefly mention the first appellate case dealing with the ACPA, \textit{Sporty's Farm, L.L.C. v. Sportsman's Market, Inc.}, 202 F.3d 489 (2d. Cir.), cert. denied, 530 U.S. 1262 (2000), in order to emphasize the significance of the bad faith intent requirement, \textit{see id.} at 498-99, and show how new this issue is—the first appellate case on the statute was just recently decided in February 2000!} In \textit{Caesars World, Inc. v. Caesars-...}
the district court countered the defendant’s constitutional challenge to in rem jurisdiction by holding that a minimum contacts analysis is not necessary when the property “seized” is the entire subject matter of the controversy. In Caesars World, the court also rejected the defendant’s other argument, that a domain name is not the proper kind of thing to serve as a res, by holding that there is no prohibition on a legislative body (here, Congress), from making something (here, data) property.

In Broadbridge Media, L.L.C. v. Hypercd.com, the Southern District of New York held that besides just the in personam arm of the ACPA requiring bad faith, the in rem jurisdiction arm also required the same bad faith intent to profit from the good will of a mark. The court found that Henderson, the owner of Hypercd.com, had the requisite bad faith intent and it granted a preliminary injunction for the transfer of the domain name to Broadbridge Media. The court found this despite the fact that it was Broadbridge Media who approached Henderson with offers of monetary compensation for selling them the domain name. The court only made cursory notice of the fact that Henderson was a Canadian, living in Canada, who registered his domain name with an American registry.

Henderson, a Canadian, lost his

121. See id. at 504. For more information regarding the relationship between in rem jurisdiction and minimum contacts, see generally Shaffer v. Heitner, 433 U.S. 186 (1977).
122. See Caesars World, 112 F. Supp. 2d at 507. But is this really so? See Network Solutions, Inc. v. Umbro Int’l, Inc., 529 S.E. 2d 80, 86 (Va. 2000) (holding that a domain name is not gamishable, and therefore not property).
124. Because the party in an in rem action is property (the website), it seems odd that the courts look to the registrant’s state of mind in an in rem action. However, the Eastern District of Virginia has indicated that a court does not need personal jurisdiction “over a registrant before it can assess whether [the] registration of . . . domain names was motivated by a bad faith intent to profit.” Heathmount A.E. Corp. v. Technodome.com, No. CA-00-00714-A, 2000 U.S. Dist. LEXIS 20316, at *11 (E.D. Va. Dec. 29, 2000), appeal dismissed, No. 01-1153, 2002 U.S. App. LEXIS 475 (4th Cir. Jan. 10, 2002).
125. See Broadbridge, 106 F. Supp. 2d at 511. The plaintiff, Broadbridge Media, argued that because it was not explicitly written into the in rem portion of the ACPA, bad faith was not required. The court held that the statute must be read as a whole, and that not requiring bad faith intent to profit from a mark in an in rem jurisdiction case would punish those who registered domain names containing the mark of others with intents other than bad faith. See id.
126. See id. at 512.
127. This provokes the argument that the “bad faith” requirement in the ACPA is too generous in favor of the mark holder. It makes sense that if Henderson had tried to extort money, such as in the Babyguin hypothetical, see discussion supra Part II.B, then that would constitute bad faith. But if the holding in Broadbridge stands, one will immediately be deemed to have satisfied the bad faith requirement if one even listened to any offer of sale, let alone haggled.
128. See Broadbridge, 106 F. Supp. 2d at 507.
website via the in rem arm of the ACPA.\textsuperscript{129} No mention was made of this fact. No mention was made of the suitability of Broadbridge obtaining relief by the UDRP in this case.\textsuperscript{130}

Another disturbing in rem ACPA case is Heathmount A.E. Corp. \textit{v. Technodome.com}.\textsuperscript{131} Heathmount involved a Canadian mark holder and a Canadian domain name owner who registered with NSI.\textsuperscript{132} The United States District Court for the Eastern District of Virginia permitted jurisdiction in Virginia and rejected the defendant website’s arguments that Canada was the more appropriate forum, or alternatively, that the UDRP should be used.\textsuperscript{133} The court stated that the UDRP is “not equivalent to the formal consideration of a cause by a court of record.”\textsuperscript{134} It continued, stating that the UDRP “does not provide parties with the procedural safeguards supplied by a court proceeding. Moreover, [the UDRP] lacks the enforcement power of a court system. For these reasons, [the UDRP] is not an adequate substitute for this court’s consideration of the issues presented here.”\textsuperscript{135}

As a result, due to the easily satisfied standards of bad faith required by the ACPA, any person who registers a domain name with a domain registry that is located in the United States\textsuperscript{136} could potentially lose that website. This poses some comity of nations problems.

\textsuperscript{129} See id. at 510.

\textsuperscript{130} Broadbridge initiated its in rem ACPA proceeding only two days after it filed its UDRP complaint against Henderson. See id. at 508. The court, rather than waiting for a UDRP determination, held that it had jurisdiction to hear the case. See id. at 509. More importantly, the court erred by stating that “paragraph 4(k) [of the UDRP stands] for the proposition that either party involved in a UDRP administrative proceeding may file a lawsuit before, during, or after the administrative proceeding.” Id. (emphasis added). The UDRP explicitly states that a UDRP proceeding “shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before [the UDRP] proceeding is commenced, or after such proceeding is concluded.” ICANN, \textit{Dispute Resolution Policy}, supra note 34, \textsuperscript{4}4(k) (emphasis added). Thus, the court misread the UDRP which plainly does not permit litigation to be commenced during the UDRP proceeding. Therefore, the court did not have jurisdiction to hear the case.


\textsuperscript{132} See id. at *1-2.

\textsuperscript{133} See id. at *16-23.

\textsuperscript{134} Id. at *23.

\textsuperscript{135} Id.

\textsuperscript{136} Most domain registries are located in the United States. See supra notes 32-33 and accompanying text. The world’s two largest registries are NSI, Inc., and Register.com, located in Virginia and New York, respectively. See Lee, supra note 1, at 126-32 (discussing in rem jurisdiction and the situs of intangible property). Therefore, for cases involving foreigners registering websites in the United States, chances are that, under the ACPA, in rem jurisdiction will place the litigation in Virginia or New York.
C. The ACPA Harms the Comity of Nations

1. The United States Has a Different Philosophy Behind its Mark Protections than Other Nations

An example of how the comity of nations is harmed is the fact that the United States has a different philosophy behind its mark protections than most other nations. Not only must an entity obtain a valid mark for its product or service, but the entity must also use the mark on the goods or services in respect of which the rights were claimed. Without use, consumers would be unable to associate the producer of the good or services with the goods or services produced, which is the very point of mark law. This is called the use-based philosophy, in which the “first producer to use the mark obtains the rights with respect to the goods upon which and geographical areas in which use occurred.” In contrast, most other nations have a registration-based system of mark priority. In these countries, the first to register a mark obtains exclusive right to use the mark on the goods or services at issue.

To exemplify the problem this can create, one needs to ask what is the geographic scope of use when a mark is used as a domain name, or a portion of a domain name? In the United States, a use-based system, has the user made use of the mark globally? In a registration-based system, where there are other users with that same mark, has that U.S. user violated and infringed upon the rights of the mark holders in those countries? This shows that there needs to be a supranational system of deciding these issues on the Internet, and this is only one issue where there could be conflicts with the way other nations treat the marks of their citizens.

2. What Law Should Govern the Internet?

If one looks to mark treaties between the nations, one does not gain too much aid in answering the question of how to deal with the domain name system and marks because these treaties are jurisdictionally based. The principal treaty on marks is the Paris Treaty, which has

138. Id.
139. See id.
140. See id.
141. An exception to this is the European Community trademark. See id. at 500 n.16.
been signed by approximately 155 nations. This treaty states that mark rights in one country are independent of mark rights in other countries. However, the treaty sought to facilitate multinational registration, to protect marks beyond the borders of the registration country if the mark is well-known in other nations, and to assure that citizens of other countries have equal ability to register marks as domestic citizens. This, however, does not provide a solution to the problem, and in fact compounds the problem of the Internet by treating marks territorially, providing no solution to a problem that has been created out of our ever increasing technology. The only way to protect a mark in all countries would be to register that mark in every country. Nevertheless, because there can only be one SLD per TLD, that still does not solve the problem concerning the Internet. So how are marks to be protected in the domain name system without the imposition of one nation's laws as the law of the entire Internet, or the opposite, total intellectual property anarchy?

Legal scholars have debated for several years whether the Internet should be self-governing or subject to the legislation of nations. On the side of self-governance of the Internet are Professors Johnson and Post, who believe that it is illegitimate for any local sovereign to set rules for global domain space (the gTLDs, such as .com, .net, etc.). If one nation were allowed to set rules for a global phenomenon, such as Saudi Arabia banning pornographic images or the online advertising or display of alcoholic beverages, these rules would have extraterritorial effects. If Saudi Arabia were to actually succeed in banning online pornography or sites pertaining to alcohol, Saudi Arabia either would have cut itself off from the Internet, or somehow got their way in the nations where the pornographic or alcohol-related content originated from. But is this fair to those outside of Saudi Arabia who wish to see pornographic images, or would it be fair to those outside of Germany who wish to access websites about Nazism, but cannot because Germany has banned such sites? These represent some of the problems that can arise when nations impose their laws into a new and global medium, such as the Internet.

143. See id. art. 6.
144. See id.
145. See id. art. 6th.
146. See id. art. 2.
On the other side of the Internet governance argument are the legal scholars who believe that a supranational system of domain name governance is actually antithetical to democracy.\textsuperscript{148} They believe this to be the case because supranational bodies that would regulate the Internet would either be semi-private organizations, such as ICANN, whose members are chosen not by the will of the people, or would be international bodies whose members are appointed by national legislatures.\textsuperscript{149} While this seems more democratic than the people having absolutely no say as to who constitutes these regulatory groups, the appointment of delegates by a legislature to an international body still creates a group of representatives that are "twice removed from the people."\textsuperscript{150} Though there are problems with both alternatives, a private entity domain name regulator or an appointed international regulatory group, either alternative would be better for comity of nations than the hegemony of one nation's laws on the Internet.

3. The Problem of Anti-Americanism
The ACPA violates the comity of nations. No matter where someone is located, if he or she registers a domain name from a domain registry located in the United States, that individual can have the domain name taken away via the ACPA's \textit{in rem} provision. This is something that needs to be avoided at all costs, or other nations will probably retaliate in some form. The problem is partially created by American arrogance, coming from the fact that the Internet happens to be an American creation, dating back to the 1960s. This arrogance is shown with respect to governance of the Internet as early as 1997. Representative Charles W. Pickering stated that "'American taxpayers, companies, and the government built the Internet. This is something uniquely American.' . . . Ceding governance to a global body 'is not going to sell very well—not here, not on Main Street.'\textsuperscript{151} One must ask the question whether Representative Pickering realizes that the Internet does not only run through Main Street, but also through the Pall Mall in London, the Kurfürstendamm in Berlin, and practically everywhere else in the world where electricity and telephone lines exist. It is not difficult

\begin{quote}
\textsuperscript{149} See id. at 1114-15.
\textsuperscript{150} See id. at 1115 (comparing this situation, where a "representative" is "only a representative of [an] elected representative["], much like how Senators were chosen prior to the Seventeenth Amendment).
\textsuperscript{151} Chandrasekaran, supra note 21, at D2 (quoting Rep. Charles W. Pickering).
\end{quote}
to see why there is so much anti-Americanism\textsuperscript{152} in the world when our leaders believe that a global phenomenon is uniquely American, and must be governed by America. How would Representative Pickering feel if the British decided that they no longer wished to share jet technology with the rest of the world because the inventor of the jet engine, Frank Whittle, was British? Representative Pickering's type of reasoning also probably affected the drafting of the ACPA, which is making American mark law the law of the Internet, and probably, because of the Internet's global consequences, the law of the entire world.

V. CONCLUSION

The Internet is borderless,\textsuperscript{153} and if one nation begins to dominate it,\textsuperscript{154} the sovereign rights of other nations could be violated.\textsuperscript{155} So, when the ACPA causes of actions are started against a non-resident of the United States, the aggrieved mark holders should be required to abide by the UDRP as their sole remedy in this limited circumstance. Though a party is free to file litigation in court under the current rules of ICANN in addition to utilizing the UDRP, ICANN should change its policy in this regard. The UDRP can adequately provide relief for complainants.

\textsuperscript{152} For a recent account of anti-Americanism, see Martin Kettle, \textit{U.S. Bashing—It's All the Rage in Europe}, WASH. POST, Jan. 7, 2001, at B4. Kettle's op-ed article in the Washington Post describes issues that bother some Europeans, including the barbarism of capital punishment, global warming, and national missile defense. Kettle's piece, written before the events of September 11, 2001, also addresses some Europeans' doubts about the presidential ability of George W. Bush, who had just been elected. \textit{See id.} The ACPA is only going to compound the problem of the rest of the world not liking us.

\textsuperscript{153} Assuming there is no firewall preventing the information from being accessed in a particular area, information located on the Internet can be accessed anywhere on Earth. For example, in Germany, because of the shame of their Nazi past, there are laws that forbid certain forms of expression, especially when it comes to Nazism. \textit{See} David E. Weiss, \textit{Note, Striking a Difficult Balance: Combating the Threat of Neo-Nazism in Germany While Providing Individual Liberties}, 27 VAND. J. TRANSNAT'L L. 899, 920 (1994). In Germany, it is forbidden to say the "Sieg heil" or give the accompanying salute. \textit{See id.} at 928. However, while those actions may be illegal in Germany, members of the Neo-Nazi movement can access information on the web that might not be legal in Germany, because those sites exist elsewhere, perhaps in Norway or in the United States.

\textsuperscript{154} \textit{See} Johnson & Post, \textit{supra} note 147, at 1367 (stating that "[g]lobal computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of laws based on geographic boundaries").

\textsuperscript{155} \textit{See} RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 201 (1987) ("Under international law, a state is an entity that has a defined territory and a permanent population, under the control of its own government, and that engages in . . . formal relations with other such entities."); \textit{see also id.} § 402 ("[A] state has jurisdiction to prescribe law with respect to (1)(a) conduct that, wholly or in substantial part, takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside its territory that has or is intended to have substantial effect within its territory.").
while still maintaining a semblance of independence from the United States. ICANN is not perfect, and neither is the UDRP. The same free speech concerns exist with the UDRP as with the ACPA, and the arbitrators deciding UDRP cases probably will be as pro-mark holder as the U.S. courts tend to be. Until a better solution comes along regarding solving international domain name disputes, the UDRP is the only existing alternative that maintains comity of nations and could also provide this nation with a well-deserved relief from the currently increasing phenomenon of anti-Americanism.

*Steven J. Coran*

* I would like to dedicate this Note to my parents because of their unconditional love and support for me. I would also like to thank Professor Linda C. McClain for her assistance and guidance in the preparation of this Note. In addition, I would like to thank the editors and staff of Volumes 29 and 30 of the Hofstra Law Review not only for their work on my Note, but also for making my law school experience pleasant.