THE ANTICYBERSQUATTING CONSUMER PROTECTION ACT: WILL IT END THE REIGN OF THE CYBERSQUATTER?

Jason H. Kaplan*

I. INTRODUCTION

Anyone who has watched television, picked up a newspaper, or stepped outside recently knows of the ever-expanding reach of the Internet. "Internet start-ups," "dot-coms," and "e-commerce," are words on the lips of every financial analyst. Online business seems to be the wave of the future . . . and the present. That is why many "real-world" businesses are scrambling to establish an Internet presence at any price. This desperation has left these businesses vulnerable to what is referred to as "cybersquatting" or "cyberpiracy."

A company's presence on the Net must start with a "domain name" as a corporate identifier.[1] Many businesses choose to use their trademarks as domain names because consumers are already familiar with those marks.[2] A trademark is any word, symbol, device, or combination thereof to identify and distinguish the *source* of one's goods or services, rather than merely the goods or services themselves.[3] Because most Internet users know that companies use their trademarks as domain names, people will often type in a company's trademark in

* J.D. Candidate, University of California at Los Angeles School of Law, 2001; B.A. Washington University, 1998.

[1] Sally M. Abel, *Trademark Issues In Cyberspace: The Brave New Frontier*, 5 Mich. Telecomm. & Tech. L. Rev. 91 (1999).

[2] For example, Nike would want to use "nike.com" to identify itself.

[3] 15 U.S.C. §1127 (Supp. 1996).

hope of finding the company's website.[4] Thus, using a product or company's trademark as a domain name makes access to a website more convenient for consumers and consequently boosts online commercial success. Without the use of an easily identifiable trademark as a domain name, the consumer must utilize an online search engine[5], or the company must promote a less recognizable domain name[6].

Today, anyone can register a domain name . . . as long as someone else has not registered that domain name first. Unfortunately, many companies have found that someone *has* already registered the domain name corresponding to their trademarks and is willing to sell it for a hefty sum. In a frenzy to jump on the Internet bandwagon, many companies have paid exorbitant amounts of money to these "cybersquatters" for the right to use their own trademarks as domain names. Many companies that have refused to pay the cybersquatters have suffered the online financial consequences. The conflict between trademarks and domain names has led to a flood of litigation and has raised many vexing legal issues.

---

[4] In *Lockheed Martin Corp. v. Network Solutions, Inc.*, the court stated:

> If a user knows or can deduce the name associated with a Web site, the user can directly access the Web site by typing the domain name into the Web browser, without having to conduct a time-consuming search. Because most businesses on the internet use the ".com" top level domain, Internet users intuitively try to find businesses by typing in the corporate or trade name as the second level domain name, as in "acme.com."

Lockheed Martin Corp. v. Network Solutions, Inc. , 985 F. Supp. 949, 952 (C.D. Cal. 1997).

[5] The court in *Panavision Int'l v. Toeppen*, 945 F. Supp. 1296 (C.D. Cal. 1996) discussed the difficulty with search engines, such as Yahoo, Lycos, Infoseek, Alta Vista, and Hotbot:

> Search engines search the Internet using "key words" selected by the searching party . . . . Key word searches will frequently yield thousands of web sites . . . . The length and success of this process is dependent upon the searching party's ability to deduce the correct key word or words and the number of other Web sites that use the same key words.

Panavision Int'l v. Toeppen, 945 F. Supp. 1296, 1299 (C.D. Cal. 1996).

[6] For example, if "www.nike.com" were unavailable, Nike would have to promote a less intuitive domain name such as "www.justdoit.com," "www.e-nike.com," or "www.nikeonline.com."

A. The Root of the Conflict

The root of the conflict between trademarks and domain names is that the allocation of each is conducted by means of two non-integrated systems administered by different types of entities, one governmental, one private.[7]

The trademark system is a legal regime directed towards the creation and protection of an abstract concept: ownership of a trademark. Because U.S. courts recognize common law rights, a party can gain trademark protection merely by using the mark in commerce. If a party wishes to perfect its rights so as to create a rebuttable presumption that it is the owner of the mark, it must file with the U.S. Patent and Trademarks Office ("PTO") in order to be placed on the federal register.[8]

The Domain Name System ("DNS") works very differently. Every computer connected to the Internet[9] is assigned a unique numeric address, or Internet Protocol ("IP"), that consists of a string of digits separated by periods. In order to ease a person's ability to remember and locate these addresses, Internet authorities also permit assignment of corresponding, user-friendly alphanumeric addresses, or "domain names," for each numeric IP address.

In the U.S., domain names are assigned by "registrars," which are private companies that are accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") to become part of the Shared Registration System ("SRS").[10] Domain names are generally

---

[7] Martin B. Schwimmer, *Domain Names and Everything Else: Trademark Issues in Cyberspace*, 569 PLI/Pat 381, 387 (1999).

[8] The PTO judges whether trademark applications qualify for protection pursuant to the Lanham Act. Decisions on applications are appealable to the Trademark Trial and Appeal Board, which is an administrative law tribunal. The TTAB's decisions are reviewable by the Circuit Court for the Federal Circuit, if the parties choose to take it that far.

[9] The Internet is a worldwide web of networked computers linked together for the purpose of automated communication between individuals, companies, governments, educational institutions, militaries, and various local computer networks. 2 Jerome Gilson, Trademark Protection and Practice § 5.11[1] (1997).

[10] In October of 1998, the United States Department of Commerce ("DoC") and Network Solutions, Inc. amended their cooperative agreement, under which NSI had been the sole registrar and registry administrator for the .com, .net, and .org top-level

assigned on a first-come, first-served basis. In assigning domain names, registrars use a multi-level system, pairing a Top Level Domain ("TLD"), such as ".com," ".net," and ".org,"[11] with a Second Level Domain ("SLD") consisting of a unique set of letters and numbers.[12] The SLD may not contain certain symbols, such as apostrophes and commas, but may contain hyphens.

Therefore, the purpose of the trademark system is to recognize and protect rights, while the purpose of the domain name system is to award a one-of-a-kind address for operation in a telecommunications network can operate. The trademark system aims to prevent legal confusion, while the domain name system aims to prevent "communication" confusion. Because the systems have different purposes and methods of implementation, conflict is to be expected.[13] The legal issue then turns on how these conflicts should be resolved.

Cybersquatting has become one of the most rampant problems in cyberspace.[14] Mere application of traditional trademark law to the new and unique problem of cybersquatters has not consistently yielded just results in the courts.[15] On November 29, 1999, in response to this

---

domains. This amendment required the establishment of a Shared Registration System ("SRS") in which an unlimited number of registrars would compete for domain name registration business utilizing one shared registry. The DoC identified ICANN, a newly-formed, private, non-profit corporation to oversee the SRS by establishing and implementing a procedure for registrar accreditation and domain name dispute resolution policy. As of May 11, 2000, ICANN has accredited 124 registrars. *ICANN's Accreditation History Page* (visited May 17, 2000), at http://www.icann.org/registrars/accredation-history.htm.

[11] Each TLD indicates a different purpose for each website. For example, ".com" indicates a business user, "..net" indicates Internet services, ".org" indicates online organizations, ".gov" indicates a government agency, and ".mil" indicates a military address.

[12] For example, "nike" is the SLD in "www.nike.com."

[13] Schwimmer, *supra* note 7, at 389.

[14] S. REP. NO. 106-140 (1999).

[15] One commentator writes: "The use of traditional trademark factors in domain name disputes has produced inconsistent results – properly favoring trademark holders in some cases, but improperly favoring [cybersquatters] in others." Danielle W. Swartz, *The Limitations of Trademark Law in Addressing Domain Name Disputes*, 45 UCLA L. Rev. 1487 (1998). A detailed analysis of this problem is discussed below.

crisis, President Clinton signed into law the Anticybersquatting Consumer Protection Act ("ACPA") in order to clarify the issue of domain name disputes for the courts.[16]

This Article seeks to explore how courts will analyze and enforce ACPA and identify the effects that ACPA will have on cybersquatters and trademark owners. Part I outlines traditional trademark law, noting the weaknesses in infringement and dilution analysis that allowed cybersquatters to avoid liability and precipitated the need for ACPA. Part I also outlines how ACPA amends trademark law and identifies the steps of analysis courts will use to analyze and enforce the statute. Part II illustrates the particular ways ACPA has been tailored to stop cybersquatters and the reasons why it will work. Part III examines the potential problems and unjust results that may be caused by ACPA, and Part IV explores some alternative solutions to these problems. The Article concludes by providing practical steps for trademark owners to follow which will help them gain protection against cybersquatters under ACPA.

II. OVERVIEW OF TRADITIONAL TRADEMARK LAW AND ACPA

A. Traditional Dilution and Infringement Analysis and the Problems in Applying it to Domain Name Disputes

There are two traditional causes of action a trademark owner can bring in order to protect a mark: trademark dilution and trademark infringement. Both causes of action have a statutory basis for its analysis in the Lanham Act. Dilution is analyzed pursuant to § 43(c) or 15 U.S.C. § 1125(c) as amended by the Federal Trademark Dilution Act ("FTDA"). Infringement is analyzed pursuant to § 43(a) or 15 U.S.C. § 1125(a).

In analyzing liability for federal trademark dilution, courts consider the following elements: 1) commercial use of a "famous" trademark; 2) use of the trademark in commerce; and 3) the likelihood that the use of the mark by the defendant will cause dilution of the mark's distinctive quality. This dilution can come in two forms. One form is blurring, or "the whittling away of an established trademark's

[16] Anticybersquatting Consumer Protection Act of 1999, 15 U.S.C.S. § 1125(d).

selling power through its unauthorized use by others upon dissimilar products."[17] The other form is tarnishment, in which the defendant uses the plaintiff's mark in an unsavory way that damages the mark's goodwill.[18]

Two main problems arise when attempting to apply dilution analysis to cybersquatting. First, dilution protection only applies to "famous" trademarks.[19] Only a certain number of marks have reached this level of heightened recognition. If a court rules that a mark is not famous, then it loses any protection against dilution without any further analysis.

The second problem with applying dilution analysis to cybersquatters is the "commercial use" requirement. Commercial use includes the use of a trademark for the advertisement, promotion, or sale of a product.[20] Offering to sell trademark-based domain names to the rightful trademark owner also constitutes commercial use.[21] Therefore, cybersquatters avoid commercial use as long as they do not use the website for the advertisement, promotion, or sale of goods, and as long as they do not make the foolish move of demanding money from the trademark owner. If the cybersquatter waits for the mark owner to make the initial offer, it seems that the cybersquatter can avoid commercial use, and thus liability under dilution analysis.

In analyzing liability for trademark infringement, the aim is to prevent the likelihood that consumers will be confused as to what goods they are buying and the damage that is subsequently caused to the

---

[17] Some courts use a multi-factor balancing test to measure blurring. "The six factors are similarity of the marks, similarity of the products covered by the marks, sophistication of the consumers, predatory intent [of the junior user (the defendant)], renown of the senior mark [mark owner], and renown of the junior user." Mead Data Central, Inc. v. Toyota Motor Sales, Inc., 875 F.2d 1026, 1031 (2nd Cir. 1989) (Sweet, J., concurring).

[18] Tarnishment arises "when the plaintiff's trademark is linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context likely to evoke unflattering thoughts about the owner's product, or for the sole purpose of promoting a competing product." Deere & Co. v. MTD Products, Inc., 41 F.3d 39, 43 (2nd Cir. 1994).

[19] See discussion of 43(c)(1) on page 12 below.

[20] *See* Ringling Bros. – Barnum & Bailey Combined Shows, Inc. v. Celozzi-Ettelson Chevrolet, Inc., 855 F.2d 480, 481-82 (7th Cir. 1988).

[21] *See* Panavision Int'l L.P. v. Toeppen, 141 F.3d 1316 (9th Cir 1998).

trademark owner. Multi-factor "likelihood of confusion" tests vary among the federal circuits, but the Ninth Circuit balances the following eight factors: 1) the similarity of the marks; 2) the proximity of the goods; 3) the marketing channels used; 4) the defendant's intent in selecting the mark; 5) the type of goods and the degree of care likely to be exercised by the purchaser; 6) the evidence of actual confusion; 7) the strength of the mark; and 8) the likelihood of expansion of the product lines.[22]

Because courts place great emphasis on "the proximity of goods" factor, infringement analysis often allows cybersquatters to avoid liability. In traditional trademark cases, proximity of goods is an accurate indicator of whether a consumer would be confused between products. However, cybersquatters have constantly used this factor as a shield from liability.[23] By simply registering or warehousing domain names without offering any goods or services on the websites, the cybersquatter will always be able to avoid liability under the proximity of goods analysis.[24]

Another problem in applying traditional trademark law to domain name disputes is the fact that cybersquatters can literally hide from prosecution. The court in *Porsche Cars North America, Inc. v. Porsche.com* held that the Lanham Act did not authorize in rem actions against the domain names themselves, even when plaintiffs could not find the domain name owners after due diligence. [25]

B. How ACPA Works

In response to the regularity with which cybersquatters avoided liability due to the courts' adherence to strict traditional trademark analysis in domain name disputes, Congress passed ACPA. ACPA provided the Lanham Act with the modernized weapons it needed to

---

[22] AMF, Inc. v. Sleekcraft Boats, 599 F.2d 341, 348-49 (9th Cir. 1979). This test is based on the test set out by the Second Circuit in Polaroid Corp. v. Polarad Electronics *Corp.*, 287 F.2d 492, 495 (2d Cir. 1961).

[23] *See* Swartz, *supra* note 15, at 1498 (discussing the pros and cons of applying trademark and dilution analysis to domain name disputes).

[24] *See* Intermatic v. Toeppen, 947 F. Supp. 1227, 1234 (N.D. Ill. 1996).

[25] Porsche Cars N. Am., Inc. v. Porsche.com, 51 F. Supp. 2d 707 (E.D. Va. 1999).

resolve domain name disputes. ACPA eliminated loopholes in traditional trademark law by providing an analytical structure specific to domain name disputes, providing protection for individuals' names, allowing in rem actions against domain names themselves, and allowing the recovery of statutory damages.

The first appellate case to rule upon an ACPA claim was *Sporty's Farm v. Sportsman's Market*.[26] In *Sporty's Farm*, the Second Circuit outlined a five-step process for ACPA analysis. First, the court must determine whether it has personal jurisdiction over the defendant or if an in rem action against the domain name itself is necessary. Second, the court must determine if the plaintiff's trademark is famous or distinctive in order to be protected under ACPA. Third, the court must determine whether the plaintiff's trademark and the defendant's domain name are "confusingly similar." Fourth, the court must determine whether the defendant acted with a "bad faith intent to profit." And fifth, the court must determine the proper remedy. Cases involving actions against registrars, actions based on misrepresentation by the plaintiff, or domain names containing names of living persons require separate analysis.

1. Jurisdiction

The court must first determine whether it has personal jurisdiction over the defendant or if an in rem action against the domain name itself is necessary. The outcome of this decision affects the remedies that a plaintiff may receive. *Cello Holdings*, in which a New York State Court claimed personal jurisdiction over a California resident, illustrates several ways in which personal jurisdiction can be established.[27] First, personal jurisdiction can be established if the defendant's activities fall within the language of the state's long-arm statute.[28] Second, personal jurisdiction can be established if a defendant purposefully avails himself of the benefits of doing business in the state by reaching out and originating contacts with the state.[29] These

[26] Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 489 (2nd Cir. 2000).

[27] Cello Holdings, L.L.C. v. Lawrence-Dahl Cos., 89 F. Supp. 2d 464 (S.D.N.Y. 2000).

[28] Id. at 470.

[29] Id.

activities include operating a commercial website that is open to citizens of the state or promoting sales internationally through the website. Third, the court in *Cello* cites *Panavision Int'l* in which the Ninth Circuit acknowledged that:

> [S]imply registering someone else's trademark as a domain name and posting a website on the Internet is not sufficient to subject a party domiciled in one state to a jurisdiction in another." See *Panavision*, 141 F.3d at 1322. The court went on to hold, however, that a defendant who "engaged in a scheme to register [plaintiff's] trademarks as his domain names for the purpose of extorting money from [plaintiff]" was subject to personal jurisdiction in the plaintiff's state.[30]

One of the most important amendments that ACPA adds to traditional trademark law is that a trademark owner can now bring an in rem action against the domain name itself when the cybersquatter is not subject to personal jurisdiction or cannot be found. This overturns the holding in *Porsche Cars*, in which the court held that the Lanham Act did not authorize in rem actions.[31] ACPA provides that a trademark owner can bring an in rem action against the domain name itself in the jurisdiction of the registrar when the domain name infringes or dilutes the owner's trademark and the owner can *neither* obtain personal jurisdiction against the cybersquatter *nor* find the cybersquatter through due diligence.[32] The due diligence requirement can be met by sending notice of the alleged violation and intent to proceed to the registrant of the domain name at the postal and e-mail address provided by the registrar, and by publishing notice of the action after filing if the court so directs.[33]

Where can a trademark owner bring an in rem action? ACPA provides:

> (d)(2)(C) In an in rem action under this paragraph, a domain name shall be deemed to have its situs in the judicial district which—
>
> (i) the domain name registrar, registry, or other domain name authority

---

[30] Id.

[31] Caesars World Inc. v. Caesars-Palace.com, *et al.*, 112 F. Supp.2d 502 (E.D. Va. 2000) was the first case to uphold an in rem cause of action against a domain name and specifically notes that *Porsche Cars* is no longer good law when in conflict with ACPA.

[32] 15 U.S.C.S. § 1125(d)(2)(A).

[33] *Id.* § 1125(d)(2)(A)(ii)(II).

that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.[34]

The remedies for an in rem action are specifically limited, compared to those actions exercising personal jurisdiction over the cybersquatter him or herself.[35] A plaintiff in an in rem action can get the domain name transferred to him or get a forfeiture or cancellation order for the domain name. A plaintiff may not get actual or statutory damages, nor attorney's fees or costs.

2. Is the Plaintiff's Trademark Distinctive or Famous?

The next three steps in ACPA analysis derive from statutory language. ACPA amends Section 43 of the Lanham Act, 15 U.S.C. § 1125 (2000), as follows:

(d)(1)(A) 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 which is protected as a mark under this section: 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;

---

[34] *Id.* § 1125(d)(2)(C).

[35] ACPA amends § 43 of the Lanham Act as follows:
(d)(2)(D)(i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall—
(I) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name to the court; and
(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

> (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; or
>
> (III) is a trademark, word, or name protected by reason of § 706 or title18, United States Code, or § 220506 of title 36, United States Code.

Thus, in order to be protected under ACPA, the plaintiff's trademark must be either famous or distinctive at the time of registration.

Determination of a mark's distinctiveness requires the balancing of many factors. In *Sporty's Farm*, the 2nd Circuit used the balancing test discussed above and set forth in Section 43(c)(1) of the Lanham Act for guidance in determining distinctiveness or fame.[36] Section 43(c)(1) provides:

> In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to –
>
> (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 are 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.

A mark which is not "inherently" distinctive can nevertheless become distinctive if it acquires "secondary meaning."[37] The Restate-

---

[36] Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 489, 497 (2nd Cir. 2000).

[37] RESTATEMENT (THIRD) OF UNFAIR COMPETITION §13, cmt. e (1995).

ment states:

> Secondary meaning only exists if a significant number of prospective purchasers understand the term, when used in connection with a particular kind of good, service, or business, not merely in its lexicographic sense, but also as an indication of association with a particular, even if anonymous, entity .... A designation that has acquired secondary meaning thus distinguishes the goods, services, or businesses of one person from those of another.

When determining whether or not a mark has acquired secondary meaning, courts should consider: the amount and manner of advertising, volume of sales, length and manner of use, direct consumer testimony, and consumer surveys.[38]

If the factors in § 43(c)(1) strongly favor the fact that the mark has attained "*super* secondary meaning," then it can qualify as a "famous mark."[39] One commentator has stated that the mere acquisition of secondary meaning to achieve trademark status is nowhere near sufficient to achieve the status of a famous mark; section 43(c) requires a great deal more.[40] Important factors indicating that a mark is "famous" include national recognition and an association with a particular source when the mark is *not* being used in connection with the particular goods or services that it identifies.[41]

Under ACPA, the level of distinctiveness or fame controls the level of protection the mark receives. If the plaintiff owns a merely distinctive mark, § 43(d)(1)(A)(ii)(I) provides that a defendant infringes a mark if he registers, traffics, or uses a domain name that is "identical or confusingly similar to that mark." If the plaintiff owns a famous mark, § (A)(ii)(II) gives wider protection, providing that the defendant must register, traffic in, or use a domain name that is "identical or confusingly similar to *or dilutive* of that mark." Finally, § (A)(ii)(III) gives special protection to any mark associated with Red Cross or the Olympics, providing that a defendant infringes if he registers, traffics in, or uses a domain name that is a trademark, word, or name which is associated with either organization.

---

[38] *See* International Kennel Club of Chicago, Inc. v. Mighty Star, Inc., 846 F.2d 1079, 1085 (7th Cir. 1988).

[39] I.P. Lund Trading ApS v. Kohler Co., 163 F.3d 27, 45 (1st Cir. 1998).

[40] 3 McCarthy § 24:91 (3d ed. 1996).

[41] *I.P. Lund Trading*, 163 F.3d at 46.

If a court determines that the plaintiff's mark is neither distinctive nor famous, the analysis ends, and the defendant is free from liability under ACPA.

3. "Confusingly Similar" Standard

If the court finds the mark distinctive, then it must decide whether the defendant's domain name is "identical or confusingly similar" to that mark. Use of a "confusingly similar" standard solves many of the problems with traditional infringement claims. In traditional infringement claims, plaintiffs needed to show a "likelihood of confusion" between the mark and the domain name through the multi-factor balancing test discussed above, in which one factor is "similarity of goods and services." ACPA now allows comparison of the domain name and the plaintiff's mark "without regard to the good or services of the parties." Thus, cybersquatters can no longer avoid liability by claiming they do not sell goods, provide services, or compete with plaintiff's business.

The "confusingly similar" standard also accounts for the unique format of domain names in comparison to traditional trademarks. For example, courts can consider that domain names are not caps-sensitive and cannot contain certain symbols, such as apostrophes, question marks, commas.[42] Courts can also disregard the fact that there is a ".com," ".net," ".gov," etc. at the end of the domain name because these are only top-level domains signifying the commercial nature of the site.[43]

The "confusingly similar" analysis is within the discretion of the court. The court in *Shields v. Zuccarini* added that direct evidence of confusion by Internet users bolsters a finding that the mark and the domain name are confusingly similar.[44]

If the mark is famous, a court can also find a domain name infringing if it is "identical, confusingly similar, or dilutive of that mark."[45] Thus, a defendant can infringe upon a famous mark if the

---

[42] *Sporty's Farm*, 202 F.3d at 492-93.

[43] Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3rd 1036, 1055 (9th Cir. 1999).

[44] Shields v. Zuccarini, 89 F. Supp. 2d 634, 639 (E.D. Pa. March 22, 2000).

[45] 15 U.S.C.S. § 1125 (d)(1)(A)(ii)(II).

registration, trafficking, or use of a domain name "causes dilution of the distinctive quality of the mark." The court will then use the FTDA analysis discussed above to determine whether the defendant's domain name either blurs or tarnishes the plaintiff's famous mark.

If a court finds that the domain name is not "identical or confusingly similar" to a distinctive mark or "identical, confusingly similar, or dilutive" to a famous mark, then the defendant is free from liability under ACPA, regardless of any bad faith intent.

4. Bad Faith Intent to Profit

If a court has concluded that the mark is distinctive or famous and that the defendant's domain name is identical or confusingly similar to that mark, the court must then determine if the defendant had a "bad faith intent to profit." ACPA does not provide a bright line rule for what constitutes a "bad faith intent to profit" as described in § 43(d)(1)(A)(i). Instead, ACPA lists nine factors to assist courts in determining when a defendant has acted with a bad faith intent to profit from the use of a domain name. However, courts are not limited to the nine factors; the factors are merely indicia that may be considered along with other facts.[46]

The statute amends Lanham Act §43 as follows:

> (d)(1)(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

[46] *Sporty's Farm*, 202 F.3d at 498.

> 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 subsection (c)(1) of section 43.
>
> (d)(1)(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.

Like most multi-factor balancing tests, determination of "bad faith intent to profit" is extremely discretionary. Several clear examples of "bad faith intent to profit" have already entered the courts. The clearest example involves the traditional "cybersquatter," a defendant with no intellectual property rights to the trademark who essentially blackmails a mark owner for the rights to the domain name.[47]

Another example is when a competitor registers a confusingly similar domain name to divert business. In *Sporty's Farm*, a rival

[47] Cases involving such a situation, like Panavision Int'l v. Toeppen, 945 F. Supp. 1296 (C.D. Cal. 1996), acted as the major precipitant for ACPA.

aviation apparel store, Omega, registered "www.sportys.com" even though it had no intellectual property rights in the domain name and was fully aware of the "Sporty's" trademark.[48] In *Bargain Bid v. Ubid*, a competing online auction site, Ubid, registered "www.barginbid.com" specifically to divert any Bargain Bid customers that happened to leave out the "a" in "Bargain" directly to "www.ubid.com."[49]

A third example is when a non-competitor registers a confusingly similar domain name in order to make money from either the sale of unrelated goods or from advertisers who pay for every click on the site. In *Shields*, the defendant deliberately registered five domain names that were confusingly similar to "www.joecartoon.com" in order to divert people who misspelled the legitimate domain name. The court ruled that the defendant possessed a "bad faith intent to profit" because, before the lawsuit, the defendant's site was filled with advertisements, many for adult sites, which paid the defendant for every time someone clicked on his page.[50]

Section 43(d)(1)(B)(ii) specifically provides a fair use defense to any defendant who can prove that he or she "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful." Therefore, a showing of fair use or "good faith" precludes the court from utilizing the nine-factor bad faith test. For example, in *Hasbro, Inc. v. Clue Computing, Inc.*, plaintiff Hasbro sued defendant Clue Computing, claiming that defendant's registration of "www.clue.com" infringed and diluted upon plaintiff's trademark of the Clue board game.[51] The court ruled that Clue Computing registration was a "legitimate competing use of the domain name," and neither infringed upon nor diluted Hasbro's trademark.[52] Also, in *Shields*, the court seems to indicate that if a defendant registers a confusingly similar domain name, but operates the site purely for purposes of protest or political speech without any commercial gain, he

---

[48] *Sporty's Farm*, 202 F.3d at 498.

[49] Bargain Bid L.L.C. v. Ubid Inc., CV-99 7598 (LDW), 2000 U.S. Dist. LEXIS 3021 (E.D.N.Y. January 3, 2000). *See also* Leigh Jones, *Federal Cybersquatter Law Survives Test*, N.Y.L.J., January 18, 2000.

[50] *Shields*, 89 F. Supp. 2d at 640.

[51] Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117 (1999).

[52] *Id.* at 133.

may fall under the fair use exception.[53] In cases like these, the defendant would also have to exhibit disclaimers so as not to "tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site," and thus avoid falling under § 43(d)(1)(B)(i)(V).

5. Damages and Remedies

If a court finds that the defendant has registered, trafficked, or used a domain name that is "identical or confusingly similar" to a distinctive or famous mark with the "bad faith intent to profit," damages and remedies must then be awarded. ACPA significantly changes traditional trademark law by giving successful plaintiffs the option of choosing traditional infringement remedies or collecting statutory damages that the court deems just. ACPA amends §§ 34(a) (15 U.S.C. § 1116(a)) and 35(a) (15 U.S.C. § 1117(a)) of the Lanham Act, which provide the traditional injunctions and damages for trademark infringements, to also apply to violations of § 43(d). Under § 35(a), a plaintiff is entitled to recover defendant's profits, any damages sustained by the plaintiff, the cost of the action, and in exceptional cases, attorney fees. If the court finds that the defendant has acted with the intent to deceive or defraud, § 35(b) entitles the plaintiff to three times defendant's profits or damages, whichever is greater, together with reasonable attorney fees.

ACPA further amends § 35 of the Lanham Act to include the option of statutory damages as follows:

> (d) In a case involving a violation of section 43(d)(1), the plaintiff may elect, at any time before final judgment is rendered by the trial court, to recover, instead of actual damages and profits, an award of statutory damages in the amount of not less than $1,000 and not more than $100,000 per domain name, as the court considers just.

Therefore, a plaintiff must choose the scheme that will provide the largest award and inform the court before final judgment is rendered.

It is important to note that monetary damages cannot be awarded retroactively. Under ACPA, courts cannot award actual damages under § 35(a) or statutory damages under § 35(d) in cases that involve

---

[53] *Shields*, 89 F. Supp. 2d at 641.

the registration, trafficking, or use of a domain name that occurred before January 1, 2000. However, ACPA provides that "a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark" in cases involving conduct that occurred before, on, or after January 1, 2000.[54]

Furthermore, ACPA limits liability to "the domain name registrant or that registrant's authorized licensee." [55]

6. Three Separate Causes of Action Dictated by ACPA

a. Protection for Living Individuals

Cases involving domain names containing names of living persons, actions against the registrar, or actions based on misrepresentation by the plaintiff each require a separate analysis under ACPA. First, ACPA provides separate and unique protection against pirating domain names that contain the names of living persons. There is no protection under ACPA for the registration or use of a deceased person's name.[56] Nor does protection for individuals' names apply retroactively to domain names registered before January 1, 2000.[57]

The liability standard for cybersquatting the names of individuals under ACPA § 3002 is as follows:

> (b)(1)(A) CIVIL LIABILITY – Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable

---

[54] ACPA amends § 43 of the Lanham Act as follows:
(d)(1)(C) In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

[55] § 43(d)(1)(D).

[56] However, under §§ 46 and 47 of the RESTATEMENT (THIRD) OF UNFAIR COMPETITION (2000), beneficiaries of deceased persons may bring right of publicity claims.

[57] ACPA provides:
(b)(4) EFFECTIVE DATE - This subsection shall apply to domain names registered on or after the date of the enactment of this Act.

by such person.[58]

Courts will have to clarify several ambiguities in the language of the statute. One commentator notes: "Because the liability standard, [the specific intent to profit] turns on the registrant's subjective intent, even someone coincidentally named Vanna White would run afoul of the law if she were to register her own name as a domain name with the intent to sell the domain name, either to the famous Ms. White or to a third party."[59] It remains to be seen whether the courts will follow this reasoning. The actus reus in the statute is "registers a domain name that consists of the name of *another* living person." Therefore, if the non-famous Vanna White were to register a domain name containing *her own* name, a court might find her free from liability whether or not she intended to profit.

It is also unclear as to *when* the defendant's "specific intent to profit" must be present. The statute merely states: "Any person who registers a domain name . . . with the specific intent to profit," which does not clarify whther the "specific intent to profit" must be present at the time of registration. Is a defendant is free from liability if he registers "www.vannawhite.com" with the intent to use it as a non-commercial Ms. White tribute page, but *subsequently* develops the intent to sell it to her or a third party?

ACPA does not only protect the names of *famous* individuals. Ordinary people can also sue under ACPA if a cybersquatter has pirated their namesake with the bad-faith intent to profit.

ACPA also provides a "work of authorship" exception for "good faith" registrants who use the domain name in affiliation with or in relation to the lawful exploitation of a work.[60] For example, if J.K.

---

[58] Intellectual Property and Communications Omnibus Reform Act of 1999, Pub. L. No. 106-113, 3002 (b)(1)(A), 113 Stat. 1501, 1501A-548 (1999).

[59] Joel Voelzke, *New Cybersquatting Law Gives Trademark Owners Powerful New Weapons Against Domain Name Pirates*, COMP. LAW., Feb. 2000, at 3.

[60] ACPA § 3002 provides:

(b)(1)(B) EXCEPTION- A person who in good faith registers a domain name consisting of the name of another living person, or a name substantially and confusingly similar thereto, shall not be liable under this paragraph if such name is used in, affiliated with, or related to a work of authorship protected under title 17, United States Code, including a work made for hire as defined in section 101 of title 17, United States Code, and if the person registering the domain name is the copyright owner or licensee of the work, the person intends to sell the domain name in con-

Rowling, author of the *Harry Potter* novels, or her publisher registers the domain name "www.harrypotter.com" with the intent to sell it to a third party should a decent offer come along, what would be the analysis?

To fall under the (b)(1)(B) exception, several elements must be met. First, the name "Harry Potter" must be "used in, affiliated with, or related to a work of authorship" which is protected under United States copyright law. This element will presumably be met, even if the *Harry Potter* books were written as works for hire. Second, the registrant of the domain name must be the "copyright owner or licensee of the work." Here, the author and publisher will most likely meet either requirement. Third, the sale of the domain name must be "in conjunction with the lawful exploitation of the work." Thus, if the domain name is being sold to a distributor or publisher who will lawfully advertise, sell, or distribute Harry Potter products, this element will be met. If the domain name were to be used for a non-related site, such as an adult website, the exception would not apply. Finally, the registration of "www.harrypotter.com" must not be "prohibited by a contract between the registrant and the named person." Therefore, this element will be met as long as Rowling or her publisher never entered into a contract with a living person named Harry Potter limiting their ability to register "www.harrypotter.com." If all these elements are met, Rowling or her publisher would be excluded from any liability under § (b)(1)(A).

One commentator, Steven Borgman, suggests that this exception is much broader than the example above. Borgman suggests that registration of a domain name containing a living individual's name will fall under the exception "as long as the registrant uses the chosen domain name for a site that includes a movie, photograph, drawing, story, play, sound recording, or other copyrightable works that relates

---

junction with the lawful exploitation of the work, and such registration is not prohibited by a contract between the registrant and the named person. The exception under this subparagraph shall apply only to a civil action brought under paragraph (1) and shall in no manner limit the protections afforded under the Trademark Act of 1946 (15 U.S.C. 1051 et seq.) or other provision of Federal or State law. Intellectual Property and Communications Omnibus Reform Act of 1999, Pub. L. No. 106-113, 3002(b), 113 Stat. 1501, 1537 (1999).

to or mentions" that individual.[61] It remains to be seen how the courts will interpret this exception.

If Rowling or her publishers fail to fall under the exception, any living person with the name Harry Potter could bring a civil action against Rowling or her publisher. The remedies that the real Harry Potter could hope to receive are limited to injunctive relief and, in the discretion of the court, costs and attorney's fees.[62]

b. Liability of Registrars

ACPA specifically limits the liability of registrars, such as Network Solutions, Inc. Registrars can avoid both injunctive and monetary liability, regardless of whether the domain name is finally determined to infringe or dilute the mark, by following the guidelines set out in § 32(2)(D)(ii). Conduct excluded from any liability is "any action of refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name, *either* "in compliance with a court order under § 43(d)," *or* "in implementation of a reasonable policy by such a registrar . . . prohibiting the registration of a domain name that is identical to, confusingly similar to or dilutive of another's mark."

However, there are three types of conduct that *will* expose registrars to injunctive relief. ACPA further amends § 32 (15 U.S.C. § 1114) of the Lanham Act as follows:

> (D)(i)(II) A domain name registrar, domain name registry, or other domain name registration authority described in subclause (I) may be subject to injunctive relief only if such registrar, registry, or other registration authority has—
>
> (aa) not expeditiously deposited with a court, in which an action has been filed regarding the disposition of the domain name, documents sufficient for the court to establish the court's control and authority regarding the disposition of the registration and use of the domain name;

---

[61] Steven Borgman, *The New Federal Cybersquatting Laws*, 8 Tex. Intell. Prop. L.J. 265, 274.

[62] ACPA § provides:

> (b)(2) REMEDIES – In any civil action brought under paragraph (1), a court may award injunctive relief, including the forfeiture or cancellation of the domain name or the transfer of the domain name to the plaintiff. The court may also, in its discretion, award costs and attorney's fees to the prevailing party.

(bb) transferred, suspended, or otherwise modified the domain name during the pendency of the action, except upon order of the court; or

(cc) willfully failed to comply with any such court order.

Registrars will only be liable for monetary damages under ACPA if plaintiffs can prove bad faith activity in in rem actions or in the registration or maintenance of a domain name.[63]

c. *Courses of Action for Legitimate Domain Name Holders*

ACPA's amendment of Lanham Act § 32 provides two courses of action to protect the rights of a domain name holder who feels that a lawsuit has been brought against him without merit. First, if the defendant proves the claim was brought on the basis of "knowing and material misrepresentation," then the plaintiff "shall be liable for any damages, including costs and attorney's fees, incurred by the domain name registrant as a result of such action," as well as injunctive relief.[64] Second, the domain name registrant may file a civil action to get declaratory judgment stating the legitimacy of the defendant's rights to the domain name.[65]

---

[63] First, ACPA amends § 43 of the Lanham Act as follows:
(d)(2)(D)(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under [in rem actions] except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.
Second, ACPA amends § 32(2) of the Lanham Act as follows:
(d)(2)(D)(iii) A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.

[64] ACPA amends § 32 of the Lanham Act as follows:
(2)(D)(iv) if a registrar... [refuses to register, removes from registration, transfers, temporarily disables, or permanently cancels a domain name] based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney's fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.

[65] ACPA amends § 32 to provide:
(2)(D)(v) A domain name registrant whose domain name has been suspended, dis-

III. How ACPA Will Stop Cybersquatters

ACPA will stop cybersquatters in five ways: 1) stripping away shields and filling in loopholes in traditional trademark analysis which previously allowed cybersquatters to escape liability; 2) providing a specific cause of action for individuals whose names have been pirated; 3) preventing cybersquatters from "hiding" from liability by allowing in rem actions against the domain names themselves; 4) making cybersquatting a much riskier practice by allowing statutory damages of at least $1,000 per domain name; and 5) facilitating the compliance and cooperation of registrars by limiting registrars' liability and encouraging them to establish their own policies to stop cybersquatting.

A. Stripping Away Shields and Filling in Loopholes in Traditional Trademark Analysis which Previously Allowed Cybersquatters to Escape Liability

ACPA creates a new cause of action with which trademark owners can protect their rights. Whereas traditional dilution and infringement analysis allowed cybersquatters too many avenues of escape from liability, ACPA closes these loopholes. Specifically, Congress, with the ACPA, amended the Lanham Act in several ways to address domain name disputes.

First, ACPA makes it much easier for *all* legitimate trademark owners to gain protection. The specific protection of "distinctive" marks only solves the limitation of dilution claims for famous marks. Previously, trademark owners had to rely on dilution claims as their primary defense against cybersquatting, since infringement claims were ineffective against cybersquatters. This forced many mark owners to attempt the difficult task of proving that their marks were "fa-

---

abled, or transferred under a [registrar's reasonable policy prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark] may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this Act. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.

mous."

Under ACPA, trademark owners now only need to prove that their marks are distinctive or have acquired secondary meaning to earn protection against bad faith registration of domain names that are "identical or confusingly similar." Additionally, ACPA provides famous marks with wider protection by protecting them against domain names that are "identical or confusingly similar *or dilutive*" to their mark.

Second, the "confusingly similar" standard no longer allows cybersquatters to tip infringement analysis in their favor. In the "likelihood of confusion" analysis for traditional infringement claims, the "proximity of goods" factor usually favored cybersquatters, allowing them to escape liability. ACPA now allows comparison of the domain name and the plaintiff's mark without regard to the goods or services of the parties. Thus, cybersquatters who simply warehouse domain names and wait for offers can no longer avoid liability by claiming they do not sell goods, provide services, or compete with plaintiff's business.

The "confusingly similar" standard also accounts for the unique format of domain names in comparison to traditional trademarks, thus defeating any claims that the marks are not similar because of the domain name format. For example, the court in *Sporty's Farm* found the domain name "sportys.com" indistinguishable from the "Sporty's" trademark, since apostrophes may not be used in domain names.[66]

However, in *Lucent Technologies, Inc. v. Lucentsucks.com*, the U.S. District Court for the Eastern District of Virginia stated that "lucentsucks.com" is *not* confusingly similar to "lucent.com."[67] The court carved out a special exception for "cybergriping" sites that register domain names in the form of "[company name]sucks.com" to provide a forum of critical commentary. While analyzing the claim

---

[66] *Sporty's Farm*, 202 F.3d at 497-98 (citing Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3rd 1036, 1055 (9th Cir. 1999)) (observing that the differences between the mark "MovieBuff" and the domain name "moviebuff.com" are "inconsequential in light of the fact that Web addresses are not caps-sensitive and that the '.com' top-level domain signifies the site's commercial nature").

[67] Lucent Technologies, Inc. v. Lucentsucks.com, 95 F. Supp. 2d 528 (E.D. Va. 2000).

under ACPA, the court said: "The likelihood of confusion is a key element when determining whether trademark infringement or dilution has occurred.... [The] average consumer would not confuse lucent-sucks.com with a website sponsored by [Lucent]."[68] The court also said that *true* cybergriping, or a "bona fide noncommercial or fair use of the mark," would indicate that the registrant did not register the domain name in bad faith.[69]

Third, the language in § 43(d)(1)(A) solves the "commercial use" problem in traditional dilution analysis by providing the actus reus as "registers, traffics in, or uses a domain name." Liability is no longer reserved only for those who sell goods or offer a domain name for compensation, as was the case under the FTDA. Under ACPA, a person need only register or use a domain name with bad faith to be liable. ACPA also specifically holds "ransoming" to be infringing activity under § 43(d)(1)(E), which defines "traffics in" as "transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and other transfer for consideration or receipt in exchange for consideration."

Fourth, the statutory language of the nine factors indicating "bad faith intent to profit" are specifically "designed to balance the property interests of trademark owners with the legitimate interests of Internet users and others who seek to make lawful uses of others' marks, for purposes such as comparative advertising, comment, criticism, parody, news, reporting, fair use, etc."[70] The first four factors suggest circumstances that indicate an absence of bad faith intent to profit, while the last five factors suggest circumstances that indicate that such bad faith exists.[71]

The first factor courts may consider is whether the defendant has any "trademark or other intellectual property rights . . . in the domain name."[72] This factor helps indicate whether a domain name registrant had a "good faith intent" to use domain name for legitimate purposes.

---

[68] *Id.* at 535.

[69] *Id.*

[70] S. REP. NO. 106-140 (1999).

[71] Peter J. Toren, *Anticybersquatting Consumer Protection Act,* INTELL. PROP. TODAY, Apr. 2000, at 30.

[72] § 43(d)(1)(B)(i)(I).

It also recognizes that although there can be only one domain name, different parties may have trademark protection for the same name, but in different geographic regions or areas of goods and services.[73] For example, if Westlaw Hotels registers "www.westlaw.com," Westlaw Legal Services cannot claim the hotel chain acted in bad faith simply because it also owned trademark rights in the domain name.

The second factor to consider is the extent to which the domain name is the same as the registrant's own legal name or a name by which that person is commonly identified, such as a nickname.[74] Congress apparently added this language in response to the well-publicized case where the owner of the Gumby and Pokey toys trademarks threatened to sue a 12-year old boy for registering "www.domainpokey.net." The boy, whose nickname is Pokey, used the website to post games and pictures of his puppy.[75] Again, the statute accounts for the phenomenon that although there is only one domain name, many parties may register without a bad-faith intent to profit.

Third, a court may consider the domain name registrant's "prior use, if any, of the domain name in connection with the bona fide offering of goods or services."[76] This factor investigates whether the domain name registrant has gained any common law trademark rights to the domain name through use. This factor protects the innocent registrant, as long as she has not caused a likelihood of confusion or attempted to profit from the goodwill of another's trademark.[77]

Similarly, the fourth factor considers the defendant's "bona fide noncommercial or fair use of the mark in a site accessible under the domain name."[78] Congress designed this factor in order to balance the interests of trademark owners with the interests of those who would make lawful noncommercial or fair uses of others' marks online, such as in comparative advertising, comment, criticism, parody, news reporting, etc.[79] However, Congress made clear that this factor was not

---

[73] Toren, *supra* note 71.

[74] § 43(d)(1)(B)(i)(II).

[75] Toren, *supra* note 71.

[76] § 43(d)(1)(B)(i)(III).

[77] Toren, *supra* note 71

[78] § 43(d) (1)(B)(i)(IV).

[79] S. RPT. NO. 106-140 (1999).

intended to create a loophole that would allow cybersquatters to avoid liability by using the website for a non-commercial use. The use must still be "bona fide." For example, under ACPA, the defendant in *Panavision Int'l v. Toeppen* who displayed scenes of Pana, Illinois under "www.panavision.com" would not have a *bona fide* non-commercial use because he was still ransoming the domain name to Panavision for an exorbitant amount of money.[80]

The remaining five factors seem to provide fact patterns that would characterize "bad-intent to profit." The closer the facts of the case are to any of these factors, the more the court can infer the defendant's bad faith. The fifth factor illustrates how a court can find that a defendant has acted in bad faith *without* the specific "intent to profit."[81] Echoing traditional trademark law, § (V) allows a court to consider diversions from the mark owner's website "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."

For example, in *Bargain Bid*, after the link from "www.barginbid.com" to "www.ubid.com" was severed, the defendant, ubid, posted such tasteless remarks as: "Coming soon! Jungle Love and Down on the Farm! Featuring: All Along the Hitching Post, Mississippi Sheep are Easy.... Remember, That's Bargainbid.com." The court concluded that the defendant's attempt to tarnish Bargain Bid's goodwill was further evidence of bad faith.[82]

The sixth factor allows the court to consider whether the defendant has offered to sell or assign the domain name to the mark owner for financial gain without having intended to use the domain name in the bona fide offering of goods or services. The court may also consider whether the defendant has shown a pattern of this behavior.[83] Congress tailored this factor to protect trademark owners from cybersquatters like the defendant in *Panavision Int'l v. Toeppen*[84] who was in the business of registering many well known trademarks as domain

---

[80] *See* Panavision Int'l v. Toeppen, 141 F.3d 1316, 318 (9th Cir. 1998).

[81] § 43(d)(B)(i)(V).

[82] *See* Jones, *supra* note 49.

[83] § 43(d)(1)(B)(i)(VI).

[84] *Panavision Int'l*, 141 F.3d at 1316.

names and selling them to their rightful owners. For example, in *Shields*, the court concluded that the defendant's mere registration of thousands of domain names with misspellings of celebrities', products', and famous websites' names was "compelling evidence of his bad faith."[85]

Congress emphasized that the "mere offer to sell a domain name to a mark owner or the failure to use a name in the bona fide offering of goods or services" is not sufficient to indicate bad faith. However, Congress also noted that "the offer to sell domain names for *exorbitant amounts* to the rightful mark owner has been one of the most common threads in abusive domain name registrations."[86]

The seventh factor that courts may consider is the registrant's intentional provision of material and misleading false contact information in an application for the domain name registration.[87] Prior to ACPA, which allows mark owners to bring in rem actions against the domain names themselves, falsification of contact information with the intent to evade identification and service of process by trademark owners was also a common thread in cases of cybersquatting.[88] It is also noted that the furnishing of false contact information must not be the result of mistake, inadvertence, or neglect.

The eighth factor courts may consider is whether the defendant has acquired multiple domain names that are identical to, confusingly similar to, or dilutive of others' marks.[89] In *Shields*, the defendant registered variations on "Joe Cartoon," "as well as thousands of other domain names, because they were confusingly similar to others' famous marks or personal names – and are thus likely misspellings of these names – in an effort to divert Internet traffic to his sites." The court said: "This conduct is compelling evidence of his bad faith."[90] This factor might help render extinct the person who makes cyber-

---

[85] Shields v. Zuccarini, 89 F. Supp. 2d 634, 640.

[86] S. RPT. NO. 106-140 (1999).

[87] § 43(d) (1)(B)(i)(VII).

[88] S. RPT. NO. 106-140 (1999).

[89] § 43(d)(1)(B)(i)(VIII).

[90] *Shields,* 89 F. Supp. 2d at 640. Examples of the defendant's domain name registrations of obvious misspellings of celebrities' names and famous marks were gwenythpaltrow.com, rikymartin.com, britineyspears.com, sportillustrated.com, mountianbikes.com, and msnchatrooms.com.

squatting a business or career.

The last enumerated factor is the extent to which the cybersquatter's domain name is or is not distinctive and famous within the meaning of the Lanham Act.[91] This factor makes it much more difficult for a cybersquatter to claim that there was no bad faith when registering a distinctive or famous domain name. This also helps protect innocent users who register common or generic words and then are sued by companies that use those words, however weak they are by trademark standards, as their own mark.

For example, in *Cello Holdings*, the defendant registered "cello.com" along with twenty other single noun names of musical instruments, such as "drums.com" and "violin.com." The court said that: "A reasonable factfinder could conclude that he did not act with an intent to 'blackmail' or 'extort' Cello, as Cello suggests. Rather, [defendant] attempted to register as domain names some twenty common nouns – names of musical instruments."[92] In denying both parties' motions for summary judgment, the court held: "Because 'cello' is a common noun, a genuine issue of material fact exists as to whether [defendant] had reasonable grounds to believe that the use of 'cello.com' was a 'fair use' or 'otherwise lawful.'"[93] Therefore, *Cello Holdings* illustrates that when one innocently registers a generic word, courts might still give the registrant the benefit of the doubt.

Finally, the court in *Sporty's Farm* emphasized that courts are not limited to these nine factors in determining "bad-faith intent to profit." The factors are, instead, merely indicia that "may" be considered along with other facts.[94] This gives the court even more flexibility to hold cybersquatters liable as they become more inventive to avoid the circumstances provided in the nine enumerated factors. For example, the court in *Sporty's Farm* noted: "The most important ground for our holding that Sporty's Farm acted with a bad faith intent . . . are the unique circumstances that do not fit neatly into the specific factors enumerated by Congress but may nevertheless be con-

---

[91] § 43(d)(1)(B)(i)(IX).

[92] Cello Holdings, L.L.C. v. Lawrence-Dahl Cos., 89 F. Supp. 2d 464, 474 (S.D.N.Y. 2000).

[93] *Id.*

[94] *Sporty's Farm*, 202 F.3d at 498.

sidered under the statute."

The defendant in this case, Omega, registered "sportys.com" in order to gain a competitive edge on Sportsman's, the trademark owner of "Sporty's." After the lawsuit was filed, however, Omega formed another company named Sporty's Farm that sold Christmas trees. The court found the defendant's explanation that the name "Sporty's Farm" was derived from a childhood memory of his dog Spo*tty* more amusing and incriminating than credible and exculpating.[95] Therefore, elaborate steps taken by cybersquatters to avoid the appearance of bad faith might result in the exact circumstances that will lead to a court's finding of such bad faith.

B. Protection for Living Individuals' Names

Since individuals usually cannot register their actual names as trademarks unless they use it in connection with the sale of goods or services, cybersquatters had much success in avoiding liability under traditional trademark analysis. However, ACPA now provides a separate cause of action specifically protecting the names of living individuals. Though several suits have been filed by celebrities under ACPA, no decisions have yet been reported, mostly due to the fact that the cases have settled out of court. This trend of settlements might indicate that because the law is so straightforward, cybersquatters of this type would have few defenses at trial and would rather save time and money by settling. Another possibility is that famous people, who might be the only people with the time and willingness to litigate the matter, have chosen to proceed under ICANN's Uniform Dispute Resolution Policy because it will provide the same results in much less time and expense.[96]

ACPA does not only protect the names of *famous* individuals. Ordinary people can also sue under ACPA if a cybersquatter has pirated their domain namesake with the bad-faith intent to profit. However, this seems like a cause of action that will seldom reach litigation, be-

---

[95] *Id.* at 499.

[96] The panel in Roberts v. Boyd (WIPO No. D2000-0210, May 29, 2000) stated that, under the UDRP, names that are sufficiently prominent so as to possess trademark rights are protected against registrants who possess no trademark rights in that name. See section IV(B) below for discussion on the speed and ease of the UDRP.

cause cybersquatters mainly register famous domain names in order to extort those celebrities for money. However, one commentator suggests that Congress tailored the statute this way to prevent "companies or individuals from scooping up large numbers of domain names in the hopes of ransoming them back to the people who happen to have those names."[97]

C. *Preventing Cybersquatters from "Hiding" from Liability by Allowing In Rem Actions Against the Domain Names Themselves*

Another way in which ACPA will stop cybersquatters is by allowing cybersquatting victims to bring in rem actions against the domain names themselves when the cybersquatters cannot be found. Allowing in rem actions provides several new advantages for mark owners. First, domain name holders can no longer hide from legitimate trademark owners, sticking their tongues out at mark owners behind the *Porshe* decision. Second, the "due diligence" standard takes little effort to meet, rendering in rem actions easy to bring if a cybersquatter runs and hides. A mark owner need only send notice to the domain holder's postal and email addresses that are listed with the registrar. Third, ACPA gives mark owners the freedom to bring in rem actions in *any* judicial district as long as the registrar agrees, either before or after the suit has been filed, to deposit the necessary documents with the court.[98] Finally, upon receipt of written notification of a filed, stamped copy of the complaint, the registrar must immediately freeze the domain name (i.e., the registrar must not transfer or cancel the registration except as ordered by the court). Thus, a cybersquatter would not be able to shut down the site or transfer the domain name to an affiliate in an attempt to avoid liability after the lawsuit has been filed.

The only disadvantage in proceeding in rem is that the court can only grant injunctive relief in the form of forfeiture, cancellation, or transfer order. Monetary damages and attorney fees cannot be awarded unless the defendant shows "bad faith or reckless disregard,

---

[97] Voelzke, *supra* note 59, at 4.

[98] *Id.* at 5.

which includes willful failure to comply with any such order."[99] However, in rem procedures are not exclusive, and mark owners can still bring a regular civil action for damages against the domain name holder in addition to the in rem action against the domain name itself.[100]

D. *Making Cybersquatting a Much Riskier Practice by Allowing Statutory Damages of At Least $1,000 Per Domain Name*

The threat of thousands of dollars in statutory damages may also put an end to cybersquatting. ACPA provides successful trademark owners the option of choosing traditional infringement remedies or collecting statutory damages that the court deems just. Before ACPA, cybersquatters were rarely required to pay monetary damages, so "even with consistent victories being won by mark owners in court, a cyberpirate's risk/benefit analysis might still generally have concluded that cyberpiracy was a profitable venture."[101] The prospect of damages of *at least* $1,000 *per domain name* and the potential for $100,000 dramatically alters that risk benefit analysis and is likely to diminish, if not end, the most egregious forms of cyberpiracy.[102]

E. *Facilitating the Compliance and Cooperation of Registrars by Limiting Registrars' Liability and Encouraging them to Establish their Own Policies to Stop Cybersquatting*

Limiting the liability of registrars, such as Network Solutions, Inc., who act in good faith helps stop cybersquatting in two ways. One way is that it ensures the cooperation of registrars, facilitating the enforcement of the law against cybersquatters. Thus, a registrar will have no fear of repercussions if it refuses to register, removes from registration, transfers, temporarily disables, or permanently cancels a domain name as long as it is in compliance with a court order or in the implementation of a reasonable policy.[103] ACPA further facilitates en-

---

[99] § 43(d)(2)(D)(ii).

[100] Voelzke, *supra* note 59, at 5.

[101] Michael D. Bednarek & John I. Stewart, Jr., *Cyberpirates, Beware*, NAT'L L.J., January 31, 2000, at C1.

[102] *Id.*

[103] § 32(2)(D)(ii).

forcement of the law by holding registrars liable for injunctive relief if the registrar *fails* to comply with court orders.[104]

Another way limiting the liability of registrars helps stop cybersquatting is by providing an incentive for registrars to implement reasonable policies to prevent the registration of infringing domain names. This clause may have anticipated ICANN's Uniform Dispute Resolution Policy ("UDRP") that was implemented on January 1, 2000 – the same date as ACPA. Though ICANN is not a registrar itself, it is the entity that oversees all registrars in the SRS; therefore, the UDRP will most certainly fall under this clause.[105]

In sum, ACPA allows trademark owners to fully protect their trademarks, even in the modern realm of the Internet. By sculpting liability standards to cover the conduct of cybersquatters and by filling in the legal loopholes which previously allowed them to escape, ACPA allows trademark owners to recover their rightful domain names and discourage future acts of cybersquatting.

VI. POTENTIAL FLAWS IN ACPA

Although ACPA was intended to plug holes in trademark law caused by the advent of the Internet, other holes may naturally have

---

[104] § 32(2)(D)(i).

[105] See discussion of UDRP below.The UDRP differs slightly from ACPA. First, it is an arbitration procedure that is intended to be fast and relatively inexpensive, taking less than 60 days and costing less that $3,000. Second, the UDRP provides remedy for statutory damages. Third, the UDRP does not have a separate cause of action for the name of living individuals. Fourth, although the UDRP also focuses on bad faith, it considers four factors:

> 1) Whether the registrant obtained the domain name to prevent the trademark owner from using its mark in a domain name and has a pattern of such conduct;
>
> 2) Whether the registrant obtained the domain name primarily to sell, rent, or otherwise transfer it to the trademark owner or the trademark owner's competitor;
>
> 3) Whether the registrant obtained the domain name primarily to disrupt the business of a competitor; or
>
> 4) Whether the registrant uses the domain name to intentionally attract Internet users for commercial gain by creating a likelihood of confusion with the complainant's mark.

For further analysis of the UDRP, see *Uniform Dispute Resolution Policy Page* (visited May 17, 2000), at http://www.icann.org/udrp/udrp.htm, and Howard Siegel and Steven R. Doran, *Chasing Down Cybersquatters Who Register Celebrity Domain Names*, ENT. L. & FINANCE, March 2000, at 1.

burst open. In its attempt to shift the balance of trademark law from the domain name registrant to the trademark owner, ACPA may in fact have shifted the balance too far. Thus, several questionable public policy and legal issues spring from this shift of power.

A. Public Policy Problems Caused by ACPA

First, one must consider the public policy issues raised by the implementation of ACPA, especially in relation to large corporations. Before ACPA became law, many large companies used the threat of lawsuits to coerce legitimate, less-wealthy domain name owners to transfer the domain name to the company. This strategy is referred to as "reverse domain-name hijacking."[106] In its weak attempt to stop this practice, ACPA provides two courses of action for legitimate domain name holders. Domain name holders have the opportunity to file a civil action to establish legitimate ownership of the domain name, and they may be awarded damages, including costs and attorney's fees for fraudulent lawsuits.[107]

These remedies seem too lenient upon those parties that bring unfounded claims. The liabilities that large companies will face, even if the registrant can actually prove misrepresentation, do not seem to shift the risk/benefit analysis against the practice of reverse domain-name hijacking. If a domain name registrant wins a civil action establishing legitimate rights in the domain name, all the court can do is reactivate the domain name or transfer the domain name back to the registrant. Therefore, the trademark owner is merely denied a set of rights it never had in the first place.

A defendant is also entitled to recover damages if he or she can prove that the lawsuit was based on "knowing misrepresentation." However, requiring "knowledge," the highest standard of mens rea, allows a plaintiff to avoid liability by only showing some small degree of merit. Even if the registrant *can* prove "knowing misrepresentation," the most he or she may receive are costs and attorney's fees. Unless a registrant conducts major e-commerce from the website, damages will probably be minimal. Furthermore, regular people and

---

106 Swartz, *supra* note 15, at 1495.

107 §§ 32(2)(D)(iv) and (v).

smaller companies would likely choose to settle or simply transfer the domain name to the larger company, rather than face a long, expensive court battle and the potential for $100,000 in statutory damages. Thus, large companies weigh the prospect of winning high statutory damages and a potentially profitable domain name against the prospect of paying the registrant's damages if that registrant can prove "knowing misrepresentation." The scales seem to tip heavily in one direction—towards big business.

One commentator suggests that ACPA will encourage more corporate bullying.[108] Mark Grossman muses: "The name of the Anticybersquatting Consumer Protection Act, is surely a bad political satire. The act has little to do with consumer protection, and more to do with protecting the behemoth companies who want to protect every conceivable variation of their name."[109]

However, before ACPA was passed, there were several instances in which the lightweight stood up to, and beat, the heavyweight. One example is the *Hasbro* case, in which Clue Computing, a small Colorado company, mounted a successful defense against Hasbro for the registration of www.clue.com.[110] Is the fortitude of Clue Computing only a brave exception to the rule? Considering the high risk of statutory damages, the answer for causes of action under ACPA might unfortunately be yes.

ACPA is not *all* good for big corporations, though. Large companies must also be aware of the pitfalls of bad publicity that might result from lawsuits against smaller parties. For example, when the online toy company eToys sued the Swiss art site etoy.com, etoy supporters caused "virtual riots," protesting, boycotting, emailing, and insulting the business tactics of eToys on Internet message boards and websites. Reacting to the bad publicity, the much larger and richer eToys dropped the lawsuit.[111] Whether it is a case of reverse domain-name hijacking or simply a case of a trademark owner trying to en-

---

[108] Mark Grossman, *New Year Brings, New Laws on Cybersquatting*, BROWARD DAILY BUS. REV., January 11, 2000, at A1.

[109] *Id.*

[110] *See Hasbro*, 66 F. Supp. 2d 117.

[111] *See generally* Craig Bicknell, *EToys Relents, Won't Press Suit*, (visited Apr. 11, 2000), at http://www.wired.com/news/politics/0,1283,33330,00.html.

force his rights, public outrage over the appearance of corporate bullying might damage business.

B. Legal Problems Caused by ACPA

The issue of whether or not to sue possible infringers leads to discussion of the first of two sources of legal chaos that may be caused by the implementation of ACPA. If trademark owners decide *not* to sue parties with similar domain names, they run the risk of allowing their mark to lose its strength and distinctiveness or even abandoning the mark altogether. In *University Bookstore v. Board of Regents*, the TTAB said that distinctiveness can be lost by failing to take action against infringers. If numerous products in the marketplace bear the same mark, the mark owner's failure to police the mark can cause it to lose its significance as an identifier of a source of goods.[112] Therefore, if a mark owner allows people to register domain names containing her trademark, the mark may be weakened or abandoned. Does this mean that a mark owner has to register every possible combination of words and letters containing her trademark? Will she have to sue everyone who has registered one of these domain names? The seriousness of this risk will be determined by how the courts qualify "failure to police."[113]

Another potential problem that ACPA fails to address is the situation where two or more companies dealing in different fields of goods or services or located in different geographical areas both have legitimate claims to the domain name.[114] Does it simply become just a first in time, first in right rule? The courts will have to answer this question without help from the language of ACPA.

---

[112] University Bookstore v. Board of Regents, 1994 TTAB LEXIS 8 (1994).

[113] The TTAB in *University Bookstore* does say that minor infringement or "creeping" use will not affect the strength of one's mark, but the owner must "police" infringements if they later become serious. *Id.*

[114] For example, if the owner of Tito's Tacos in New York and the owner of a different Tito's Tacos in Los Angeles both wanted to register TitosTacos.com, both have a legitimate claim to the domain name.

V. ALTERNATIVE METHODS OF PROTECTION AGAINST CYBERSQUATTING

A. Possible Ways to Improve ACPA

There are several ways to amend ACPA that might solve the problems mentioned above. First, there must be steeper punishments for plaintiffs that practice reverse-domain name hijacking by using the threat of frivolous lawsuits. The requirement of "knowing and material misrepresentation"[115] is simply too high of a standard to meet. Perhaps, in order to receive injunctive relief and damages, an innocent user should only have to prove the lawsuit was brought negligently, or that the plaintiff *should* have known that the claim had no merit. Furthermore, for defendants that *can* prove "knowing misrepresentation," the court should be allowed to award punitive damages against the plaintiff. Wealthy trademark owners will then have a major economic disincentive to practice reverse-domain name hijacking.

Second, ACPA should be amended to clarify trademark abandonment in the context of domain names by redefining the limits of "failure to police a mark." A reasonable amendment might provide that failure to sue another who has merely registered a domain name containing one's mark would not indicate abandonment, nor would it weaken the mark's strength or distinctiveness. However, following notions of trademark law, if a plaintiff allows the domain name registrant to use the website in a way in which the domain name itself begins to gain distinctiveness, then the plaintiff's mark may in fact be weakened. An amendment defining the extent to which the mark owner must go to protect or police his mark would also be helpful. With so many different ways to letter a domain name, combined with the different .com, .net, and .org gTLD's a mark owner should not be forced to register a myriad of domain names simply to protect a single trademark. Nor should he be forced to sue every person who happens to register some variation of the trademark in a domain name.

Finally, ACPA should be amended to clarify the desired result in lawsuits involving two or more parties with *legitimate* ownership of the same trademark. Since trademarks can be confined by region,

---

[115] § 32(2)(D)(iv).

goods, and services, several parties may own the same mark.[116] ACPA should be amended to indicate whether there should be some sort of shared system or whether it is merely a first come, first served basis amongst legitimate trademark owners.

B. ICANN's Uniform Dispute Resolution Policy as an Alternative

Perhaps ICANN has already implemented a better way than ACPA to resolve domain name disputes. Since ACPA and ICANN's UDRP ("the UDRP") went into effect in January 2000, thousands of trademark owners have opted to use the UDRP rather than ACPA. A comparison between the UDRP and ACPA clearly indicates why many plaintiffs favor the UDRP.

First, an apparent advantage to the UDRP is that is intended to be fast and relatively inexpensive. Because the rulings are made by either a single or three-member panel, much of the legal red tape is avoided. The entire proceeding, from the filing of the complaint to the panel's decision, is designed to take no longer than approximately 60 days. Moreover, the complaint forms are fairly simple to fill out and are even available online, and the processing fees are no more than several thousand dollars. There are also no jurisdictional issues with the UDRP because the domicile of the trademark owner, cybersquatter, and registrar are irrelevant.

However, the speed and ease of the UDRP process may not be preferable for everyone. Those needing an *immediate* remedy may need to proceed under ACPA because the UDRP does not provide for temporary restraining orders. Although, it may take several months for a final resolution, a TRO from filing an ACPA complaint may prevent any further damage from being committed during the trial. Furthermore, because the only pieces of evidence the UDRP panel may look at are the trademark owner's complaint, the registrant's response, and possibly a reply from the trademark owner, cases with material factual disputes may be better served in a trial setting.

Second, the remedies provided under the UDRP are limited in comparison to ACPA. Simply stated, the UDRP allows either the transfer or cancellation of the domain name, but, unlike ACPA, does

---

[116] *See Hasbro*, 66 F. Supp. 2d 117.

not allow recovery of statutory damages. This might be another effect of the limited factual inquiry.

Third, the UDRP does not provide the finality that a trial decision under ACPA would provide. The UDRP allows a domain name registrant to file a lawsuit against the complainant, even after the panel has rendered a decision. The mere filing of the complaint automatically halts the domain name transfer and allows the registrant to keep the website running until the court decides who the rightful owner of the domain name shall be. Therefore, in disputable cases or cases involving a determined domain name registrant, a plaintiff may be better served proceeding directly under ACPA to prevent relitigation.

Fourth, the UDRP's treatment of living individuals' names is different from treatment under ACPA. While ACPA provides a cause of action to *any* living individual whose name has been registered, the UDRP protects only names that are sufficiently prominent so as to possess trademark rights.[117] Essentially, the UDRP only protects famous names.

Finally, like ACPA, the UDRP also focuses on bad faith, but only considers four factors:

(1) Whether the registrant obtained the domain name to prevent the trademark owner from using its mark in a domain name and has a pattern of such conduct;

(2) Whether the registrant obtained the domain name primarily to sell, rent, or otherwise transfer it to the trademark owner or the trademark owner's competitor;

(3) Whether the registrant obtained the domain name primarily to disrupt the business of a competitor; or

(4) Whether the registrant uses the domain name to intentionally attract Internet users for commercial gain by creating a likelihood of confusion with the complainant's mark.

In sum, while the liability standard for both the UDRP and ACPA are very similar, a trademark owner's decision on which way to proceed will depend little on the facts of the case and more upon which system's administration will provide more of an advantage. Early results of UDRP hearings show that over 75% of the disputes are de-

---

[117] Roberts v. Boyd (WIPO No. D2000-0210, May 29, 2000).

cided in favor of the trademark owner, leading some to say the UDRP is big business and trademark-friendly. However, when one looks closer, over 50% of these decisions are based on the fact that the registrants do not file responses. Some also point to the fact that the UDRP panels have also uniformly decided against cybergriping or [company name]sucks.com sites. However, in *Cabela v. Cupcake Patrol*, the panel notes that a "legitimate noncommercial or fair use of the domain name . . . in order to express opinions or to seek opinions of others," would indicate a lack of bad faith.[118] The reason for consistent verdicts against the alleged cybergripers, the panel notes, is that the websites were not truly being used for cybergriping; they were simply being ransomed and unused. Therefore, despite its reputation for favoring trademark owners, the UDRP may be a legitimate, fair, and effective alternative to ACPA.

C. Possible Ways to Improve the Domain Name System

Instead of simply attempting to force the "square peg" of trademark law into the "round hole" known as the Domain Name System ("DNS"), perhaps a more efficient way to solve the problem is to reshape the system. If the DNS can be broadened while maintaining its user-friendliness, then the grip of cybersquatters may be loosened and the conflict between multiple legitimate trademark owners may be solved. One of the most discussed transformations of the DNS is the addition of new generic top level domains, such as ".arts," ".shop," ".store," ".news," ".sex," ".rec," and ".firm."[119] Some argue that the addition of new gTLD's will help relieve perceived scarcities in existing name spaces and will provide consumers with a diversity of choices and options. Also, new gTLDs are technically easy to create. Those opposed to the idea argue that this will *create* consumer confusion and increase the opportunities for trademark infringement and cybersquatting.[120] However, now that ACPA provides such a strong disincentive for cybersquatters, the increase of gTLD's would seem to open opportunities to trademark owners who desire an online presence

---

[118] Cablea's Inc. v. Cupcake Patrol (NAF FA0006000095080 August 29, 2000).

[119] *ICANN's Frequently Asked Questions Page* (visited May 17, 2000), at http://www.icann.org/general/faq1.htm.

[120] *Id.*

more than it will expose them to the risk of cybersquatting.

A second possible way to restructure the DNS would be to form directories or gateways.[121] Under this system, multiple individuals or organizations could coexist under the same domain name. When someone types in the domain name, they would find a "gateway," or list of websites under that name accompanied by a description of each, giving the person the choice of which site to visit. While this system may slightly weaken an organization's ability to create a distinctive online identity, it would also prevent a cybersquatter from tying up the domain name simply by registering it.

Another possible way to avoid trademark conflicts over domain names would be to create a system of random numbers that would remove trademarks from the domain name altogether.[122] By assigning domain names as random numbers and allowing consumers to find them through a detailed directory, domain name disputes would be a thing of the past. However, this system would all but eliminate the user-friendliness of the current system to which people have firmly grown accustomed. This also seems like an unlikely alternative when one considers that Congress went to the trouble of passing ACPA in an effort to govern the "vanity name" component of the DNS as it is now.

In sum, the addition of new gTLD's and/or gateways, in conjunction with ACPA, might allow more organizations and trademark owners to join the online community and offer consumers more choices, while weakening the cybersquatter's ability to stranglehold domain name registrations.

VI. CONCLUSION

Having analyzed claims under ACPA, as above, the question for trademark owners becomes: "How can I get ACPA to work for me and what steps should I take to protect myself against cybersquatters?" By consulting with counsel to take the following steps, individual or organizational trademark owners can protect their rightful

---

[121] *See* Jennifer Golinveaux, *What's in a Domain Name: Is "Cybersquatting" Trademark Dilution?*, 33 U.S.F.L. REV. 641, 669 (1999).

[122] Bednarek & Steward, *supra* note 101.

domain names and strengthen any potential ACPA claims against cybersquatters.[123] First, a mark owner should register her trademark with the U.S. Patent and Trademark Office.[124] Second, she should register or apply to register her *domain name* as a trademark with the U.S. Patent and Trademark Office.

Third, a mark owner should document her bona fide selling of goods and services or intention thereof in connection with the mark on the website. This will specifically negate one of the "bad faith" factors[125] and present a strong defense against any challenges to her registration of the domain name.

Fourth, she should search all present registered and unregistered trademarks and service marks similar to hers and identify any accompanying domain names. She should visit those sites and any should maintain a hard copy of any pages showing whether or not the domain name is being used for a bona fide offering of goods or services. Despite the publicity generated by ACPA, some cybersquatters still admit on their pages that the domain name is available to the highest bidder. Obtaining documentation of this before the cybersquatter can change it will be extremely helpful to a subsequent lawsuit. Fifth, a mark owner should collect and document any explicit or implicit offers that have been received from cybersquatters to sell their domain names. Evidence of one's intent to sell a domain name without using it for bona fide commerce is evidence of a "bad faith intent to profit."[126] Finally, a mark owner should study the terms of ACPA and compare it to ICANN's UDRP to see if one standard of liability favors her case over the other.

What steps should then be taken if the trademark owner decides to file a cause of action under ACPA?[127] One should start by identifying and contacting the domain name registrant through the information provided to the registrar. Next, one should contact the registrar of the disputed domain name and ask to deposit the appropriate documents in

---

123 *See* Voelzke, *supra* note 59, at 6.

124 According to §§ 1 and 2 of the Lanham Act.

125 § 43(B)(i)(II).

126 § 43(B)(i)(VI).

127 *See* Voelzke, *supra* note 59, at 6.

the court of the mark owner's choosing.[128] Most registrars will probably be willing to do so. If the registrar agrees, one can file the action in the venue of her choice. If the registrar does not agree, the suit will have to be filed in the judicial district in which the registrar is located.[129]

Then, a mark owner should send notice via mail and email to the infringing domain name holder, notifying him of the filing of an in rem action against the domain name under ACPA. Notice of the action should be published, should the court direct so after filing. This conduct will meet the due diligence requirements needed in order to file an in rem cause of action.[130]

After this, a mark owner should file both an in personam action naming the individual domain name holder as defendant and an in rem action against the domain name itself. Finally, a file stamped copy of the complaint should be immediately delivered to the registrar. This will force the registrar to freeze the domain name, thus preventing the domain name from being sold or transferred before the court can make its decision.[131]

Because ACPA is so specifically tailored to the tactics and technology involved in cybersquatting, cybersquatters can no longer hide behind legal loopholes in trademark law. Those who thought they were being entrepreneurs by stockpiling others' rightful domain names in the early days of the Web have to start emptying their warehouses. No longer can cybersquatters feed off of "bad faith" and consumer confusion and ignorance for their personal gain, for ACPA has carefully tipped the scales in favor of trademark owners. Whether the scales have been tipped too far remains to be seen. Perhaps the only question left to be posed is: "As a cybersquatter, what is the quickest way for me to put my domain name into the hands of its rightful owner?"

---

[128] Under § 43(d)(2)(C)(ii), "a domain name shall have its situs in the judicial district in which documents sufficient to establish control and authority regarding the disposition of the registration an use of the domain name are deposited with the court."

[129] § 43(d)(2)(C)(i).

[130] § 43(d)(2)(A)(ii)(II).

[131] § 43(d)(2)(D)(i).