Vanderbilt Journal of Entertainment & Technology Law

Volume 7
Issue 1 *Issue 1 - Winter 2004*

Article 7

2004

Typosquatters, The Tactical Fight Being Waged by Corporations, and Congress' Attempt to Fight Back in the Criminal Arena

David A. Gusewelle

Typosquatters, The Tactical Fight Being Waged by Corporations, and Congress' Attempt to Fight Back in the Criminal Arena: *U.S. v. Zuccarini.*

By David A. Gusewelle*

While the Internet is one of the greatest technological advances in history, it has arguably been accompanied by an equally great setback: online pornography. Pornography has become nearly impossible for Internet surfers to avoid. According to a September 23, 2003, press release, the number of pornographic websites has increased 1800% since 1998 and has jumped from 28 million in 1998 to a staggering 260 million pages.[1] In fact, more than 28 million new pornographic pages were created in July 2003 alone.[2] While the advent of the Internet has brought with it countless advances, the incredible number of pornographic and obscene websites is considered by many to be the Internet's black-eye. Today, offensive material is no longer confined to the counters of disreputable stores.

> "Considering the increasing number of children who surf the Internet unsupervised at a young age and the proliferation of these websites, prevention has become a major issue."

While most types of obscene material are protected under the First Amendment of the Constitution, such protection is not without limits. For example, the transfer of obscene materials to minors under the age of sixteen years is outlawed under the U.S. Code.[3] Although children cannot be sold pornography in stores, they can still readily find it on the Internet. It has been estimated that over 90 percent of children between the ages of eight and sixteen have been exposed to obscene material on the Internet.[4] Further, the Kaiser Family Foundation found that about 70 percent of teens have come across pornography *by accident* via the Internet.[5]

While the statistics are staggering, the results of the studies will not surprise Internet users. Many pornographic websites lure unsuspecting guests to their sites through domain names which contain no references to obscenity.[6] In some instances, Internet users alarmingly stumble into pornography by misspelling the name of an actual website they desire to visit. This problem is particularly bad when the websites are those which children frequently visit. When an Internet user makes one of these mistakes, and different website appears, they have likely come across a "typosquatted" website.[7]

Typosquatting is a form of "cybersquatting." A cybersquatter is a party who possesses no legitimate interest in a trademark and attempts to profit by registering the trademark as a domain name before the rightful trademark owner can do so.[8] Cybersquatters usually attempt to resell or license the domain name back to the company that spent millions of dollars expanding the trademark's goodwill.[9] A website is typosquatted whenever an advertiser or competitor deliberately registers websites with common misspellings in their names

to drive unwilling customers to his or her digitally hijacked websites.[10] A smart typosquatter will seek out websites which are very popular and have heavy traffic.[11] He will then register domain names that users are most likely to access due to typographical errors.[12] For instance, knowing that the two names look nearly identical on first glance and that mistakes are commonly made by Internet users, a typosquatter might register the name "mircosoft.com" to attract users desiring to visit microsoft.com.

Considering the increasing number of children who surf the Internet unsupervised at a young age and the proliferation of these websites, prevention has become a major issue. Typosquatters have realized that children are much more likely to make spelling errors than adults and have started to prey on them as a newfound source of income.[13] Typosquatters now register misspellings of names that children would be likely to visit, such as Nickelodeon,[14] and redirect them to websites containing spam and offensive material. To fight this problem, parents can install software that blocks most offensive websites from their children. Congress recently stepped into the arena as well and took multiple measures against cybersquatters to re-strengthen corporate trademarks. The first major step was the Anti-Cybersquatting Consumer Protection Act (ACPA).[15] The ACPA was the first all-encompassing statutory law to fight cybersquatting.[16] Although it provides some protection, prevention by the trademark holders is really the most effective counteractive measure to typosquatters.

Congress also recently joined the fight against typosquatters who lure children to pornographic websites by enacting the Truth in Domain Names Act (TNDA).[17] The TDNA marks the first criminal statute against cybersquatters.[18] Shortly after its passage, the Department of Justice, through the TDNA, tallied its first criminal indictment against a typosquatter for registering misspellings of dozens of popular children's websites, including "Teltubbies.com," easily mistaken for "Teletubbies.com," and "Bobthebiulder.com," a typo of "Bobthebuilder.com."[19] The case was filed through the Federal Trade Commission against John Zuccarini, one of the most prolific and well known typosquatters.[20] Zuccarini has been charged multiple times for his roles in creating thousands of domain names since the late 1990's.[21] However, rather than facing civil damages for his actions, Zuccarini pled guilty.[22] He admitted to 49 counts of using domain names to direct minors to nude or sexually explicit content and was sentenced to 30 months in jail.[23] Because cyber-scammers preying on children now potentially face a jail sentence, the outcome in *U.S. v. Zuccarini* will likely have resounding effects on how pornography is disseminated to children, and the typosquatting practice as a whole.

Part II of this Note presents an overview of domain names as well as a general overview of cybersquatting and trademarks. Part III analyzes some of the measures Congress has taken against cybersquatting and the case law under those measures. Part IV gives a general overview of typosquatters, who constitute a subgroup of cybersquatters. Part V discusses the TDNA and issues that have been addressed through *U.S. v. Zuccarini*. Part VI asks whether the TDNA is an unconstitutional restriction on free speech. Part VII questions whether criminal liability is appropriate and argues for a higher culpability standard in § 2252(B)(b) of the TDNA. Finally, Part VIII proposes several options that can be used to circumvent typosquatted websites and examines the future of typosquatting after the U.S. Supreme Court's recent holding in *Ashcroft v. American Civil Liberties Union*.[24]

I. Cybersquatting Generally

A. Domain Names and Trademarks

It is no surprise that "[N]early everyone in the industrialized world . . . recognizes the [phrase], www.(fill in this blank).com."[25] This "blank" is at the heart of the domain name.[26] The alphabetical address can be almost any combination of characters, making it feasible to use one's trademark or name as the address of a website.[27] A domain name is the Internet equivalent of a telephone number or street address.[28] In short,

> [a] domain name is an easy-to-remember replacement for an Internet address. When an individual or corporation registers for a domain name, it is actually assigned an Internet Protocol (IP) address such as 169.229.97.112. ... Because IP addresses are difficult to remember, Internet users substitute unique "domain names" as pseudonyms for the computer's real identification number. When a domain name is entered into a computer it is automatically

converted into the numbered address, which contacts the appropriate site.[29]

Today, millions of domain names have been registered by businesses and individuals for websites where Internet users can find products, services, information, and pornography.[30] Internet domain names, unlike telephone numbers, convey a meaning that is independent of their function. They have two major functions: (1) to identify a particular site in cyberspace and (2) to facilitate a web or e-mail user's ability to find that site on the Internet.[31] It is the latter function that is tainted by typosquatters. This is largely because "A domain name registered to a person or business matching that party's well known trademark or company moniker will be much easier to remember and easier to grasp intuitively. These characteristics in a domain name will result in a greater number of users visiting that particular web site for the desired reasons."[32]

A trademark is defined as "a word, phrase, logo, or other graphic symbol used by a manufacturer or seller to distinguish its product or products from those of others."[33] Trademarks are often an "important tool [that] manufacturers and service companies use to distinguish their products and services from those of their competitors . . . and to influence consumers' purchasing decisions."[34] Trademark owners often assume that incorporating their mark into their domain name will ensure consumer access and promote their business. This is because "[t]he use of a recognizable company trademark or name is enhanced by the 'search and locate' nature of the Internet."[35] Thus, if Internet users know either the domain name of an IP address or a desired website, they can contact that site with relative ease.[36]

Many courts generally agree that "domain names that mirror corporate names or marks may be valuable corporate assets because they facilitate communication with the customers."[37] Domain names are both "the key to accessing information on the Internet and the key to a company's ability to achieve commercial success on the Internet."[38] Some domain names that are comprised of famous marks or other attractive generic terms sometimes can be valued at several million dollars.[39]

> "Because registration for domain names has always been on a "first come, first served" basis, individuals who were fast enough could register domain names before the mark owners had the opportunity to do so."

As the Internet grew in the 1990s, many corporations began registering their marks as domain names on the Internet. As more and more commerce flowed through the Internet, the value of domain names rose.[40] Because registration for domain names has always been on a "first come, first served" basis, individuals who were fast enough could register domain names before the mark owners had the opportunity to do so.[41] Upon securing ownership of the names, many would then attempt to sell them to the owners who often spent millions of dollars developing the goodwill of the trademark.[42] "Possessing a trademark [however] does not automatically trigger ownership or . . . use of the same word or phrase as a domain name."[43] A trademark owner must register their trademark with the Internet Corporation for Assigned Names and Numbers (ICANN), created by the Department of Commerce in 1998, to secure ownership and use.[44] In general, while courts have not held that the mere registration of a trademark as a domain name constitutes infringement *per se*, suits against these so called cybersquatters are valid and courts have enforced injunctions against such use.[45]

B. Cybersquatting

To fully understand typosquatting, one must first be familiar with cybersquatting. Cybersquatting "consists of registering, trafficking in, or using . . . Internet addresses that are identical or confusingly

similar to [protected] trademarks."[46] Registrars do not check whether applicants possess the right to use the trademark as a domain name."[47] Rather, for the application to be approved, applicants merely need to make a good faith claim to the domain name.[48] This registration system has left unethical parties, such as cybersquatters, with the necessary leeway to prevail over a rightful trademark holder in the registration process; they can take the domain name hostage and request compensation from the trademark holder.[49] Due to this low standard for registration, cybersquatting has become a major problem for trademarked entities attempting to run informational, charitable, and profitable websites on the World Wide Web. This problem has been summarized numerous times:

> Fundamentally, cybersquatters threaten the most basic objectives of trademark law, which is "reducing the customer's costs of shopping and making purchasing choices." An item bearing a trusted trademark allows a purchaser to easily and immediately determine that item's quality, history, and dependability. Trademark law ensures that a producer, and not its competitor, will receive the financial and reputation-related rewards linked with a desired product. Domain name infringement by cybersquatters weakens the fundamental trademark principle of consumer protection by permitting ruthless competitors to benefit from the mark holder's good will and reputation.[50]

As cybersquatting evolved into an international phenomenon, many squatters continued to register domain names in the U.S. partly because, prior to 2003, there was no criminal statute in the U.S. against cybersquatters.[51] Without one, corporations were essentially left with three viable alternatives to protect their trademarks. Corporations could: (1) simply ignore the problem and hope that Internet surfers would recognize that they misspelled their websites; (2) file a civil action against the squatter under 15 U.S.C. § 1125 in hopes of acquiring the address and possibly remedies; or (3) pay the squatter to turn over legal possession of the domain name to the trademark holders.[52] Because of the lengthy nature of civil litigation and the fact that restitution usually only meant turning the rights of the website over to the trademarked corporation and paying a small fine, cybersquatting became a very profitable industry by the late 1990's. In practice, none of these options proved to be an efficient way to fight the growing fire.

i. Ignoring the Problem: A Costly Mistake

Ignoring cybersquatters was initially a good option for corporations. When the Internet was still young, corporations often needed to register only one domain name. If someone mistyped it, or could not find it, they would simply use search engines to make it to the corporate website. However, as squatters added advertisements and "mousetraps" to their websites, corporations could not stand by idly. If mousetrapped at a domain name, Internet users usually "find themselves barraged with advertisements and unable to get out of the website they originally accessed."[53] They cannot leave because the windows which "pop up" automatically re-spawn whenever the user attempts to delete them. Often, those advertisements contain pornographic material or links to other undesirable sites.[54] Without taking action, it would be possible for consumers to associate the advertisements and crude material with the corporation, potentially destroying a company's goodwill.

ii. The Origins of Civil Actions Against Cybersquatters

Initially, corporations were able to defend their domain names most effectively by filing a civil lawsuit in federal court. If they wanted to sue for infringement, they "had to file a claim under the Lanham Act[55] or the Federal Trademark Dilution Act (FTDA)[56]."[57] The Federal Trademark Act of 1946, more commonly referred to as the Lanham Act, gives Congress the power to protect proprietary names against unauthorized use.[58] Under the Lanham Act existed three categories of infringement: (1) trademark infringement, arising under [§] 32; (2) confusion of source infringement, arising under § 43(a); and (3) dilution of a famous mark, arising under § 43(c).[59]

Trademark infringement actions are appropriate when trademark owners fall victim to an outside party using a domain name which bears their licensed trademark to offer similar or competing goods as the trademark holder.[60] First time visitors to the website could then easily be deceived into buying the competitor's product, or purchasing out of frustration since they could not easily locate the actual, trademarked website.[61] The competing website can also cause consumers to stop searching for the product.[62] Consequentially,

the owners of the trademark can lose substantial business opportunities that are otherwise available as a result of their trademarks.[63] Until new legislation was passed in 1999, federal courts relied heavily on this section in coming to resolutions.[64]

The most popular method for trademark holders to fight cybersquatting was through the Federal Trademark Dilution Act.[65] Unlike the trademark infringement rule, the FTDA does not necessitate a finding of likelihood of confusion, which is a requirement under § 32 of the Lanham Act.[66]

> "In 1999, Gateway bought the rights to the domain name "www.gateway2000.com" for over $100,000 from a web-squatter who was redirecting the site to pornographic material."

The FTDA provides injunctive relief to an owner of a famous or distinctive mark as against another person's commercial use of that mark when that other person's use serves to dilute the distinctive quality of the mark. [67]

iii. Adding Insult to Injury: Paying Off Cybersquatters

While paying off blackmailing cybersquatters is typically a last resort, it nonetheless happens regularly. Trademark holders often pay significant sums to cybersquatters (who own no rights whatsoever in the trademark) in exchange for domain names to avoid hassle or the potential expense of litigation.[68] In 1999, Gateway bought the rights to the domain name "www.gateway2000.com" for over $100,000 from a web-squatter who was redirecting the site to pornographic material.[69] This can lead to a highly destructive circular pattern: paying off squatters gives them additional resources with which to register new domain names. Moreover, the profiting squatters have additional incentives to continue to blackmail trademarked companies into future settlements.

II. Congress Fights Cybersquatters: The ACPA and UDRP

As cybersquatting developed in the early 1990's, Congress gradually passed responsive legislation.[70] However, as the situation became increasingly more problematic in the late 1990's, an immediate answer was needed.[71] In late 1999, two instruments were established: the Anticybersquatting Consumer Protection Act (ACPA), enacted by the U.S. Congress, and the Uniform Dispute Resolution Policy (UDRP).[72] Although these instruments did not solve some of the more crucial questions, such as which governing entity should regulate cybersquatting, Congress recognized the severity of the problem and took the first major step to deter cybersquatting.

A. The Anticybersquatting Consumer Protection Act

Recognizing that cybersquatters altered their tactics to avoid infringement and dilution violations, Congress amended the Lanham Act by enacting the ACPA. The goals of Congress in passing the ACPA included "protecting consumers and American businesses...promoting the growth of online commerce, and...providing clarity in the law for trademark owners."[73] Under the ACPA, to deter cyberquatters and to compensate trademark owners, Congress provided an award of statutory damages for defendants who acted in bad faith.[74] The most recent version of the ACPA is encoded in 15 U.S.C. § 1125(d), which governs cyberpiracy. [75] It assigns liability through civil actions if someone has a bad faith intent to profit directly through their actions and registers a domain name which is

identical or confusingly similar a trademark, word, or name protected by a trademark.[76]

In response to the new laws, cybersquatters went global, registering domain names from across the world. Doing so allowed them to avoid being subject to personal jurisdiction in the United States through the minimum contacts test.[77] In addition, ICANN devised a Uniform Dispute Resolution Policy (UDRP) in October 1999 as an alternative form of dispute resolution to combat cybersquatting.[78] UDRP litigation can be initiated if a trademark owner believes that another party infringed on his trademark by registering it as a domain name.[79]

III: A New Spin on Cybersquatting: Typosquatters

A. Typosquatters Generally

Today, although most domain names that coincide with trademarked names have been registered, there is a growing market for typosquatters. Typosquatting is the registration of domain names that are minor typographical variations on well-known names in which the registrant lacks any legal right.[80] Usually these are misspellings or incomplete names.[81] Depending on the popularity of the website, it is common for typosquatters to register dozens of variations in hopes of getting traffic to their websites.[82] They count on typing errors to divert users to their sites, where they typically lock the users in "mouse traps," causing them to view advertisements from which they profit.[83] There are three common characteristics to most typosquatted domain names. First, many registrations feature invalid Whois[84] data, failing to report the name and contact information of the domain's registrant.[85] Second, many unexpectedly provide sexually explicit content, even though their domain names do not suggest the availability of such content.[86] Finally, many "mousetrap" the user into the site, by blocking the operation of the web browser's "Back" and "Close" commands, as well as featuring multiple pop-up advertisements which automatically flood the user's computer with new windows faster than they can be deleted.[87]

B. The FTC Scores a Victory Under the ACPA: *Shields v. Zuccarini*

John Zuccarini is one of the most famous typosquatters. At his peak in late 2003, he had more than 8,800 domains registered to him or his various companies.[88] In 2001, the Third Circuit of the United States Court of Appeals held that typosquatting is a violation of the ACPA.[89] In *Shields v. Zuccarini*, the plaintiff was a graphic artist who designed, exhibited, licensed, and marketed the Joe Cartoon animated creature for more than fifteen years.[90] He created a website in June 1997 using the domain name Joecartoon.com. In November 1999, Zuccarini registered five variations on the website, including Joescartoon.com.[91] Visitors were mousetrapped into the defendant's websites whenever they misspelled the domain name.[92] In October 2001, the FTC brought suit against him, challenging his "copycat" web addresses, as well as his mousetrap techniques that prevented Internet surfers from exiting his sites.

> "They count on typing errors to divert users to their sites, where they typically lock the users in "mouse traps," causing them to view advertisements from which they profit."

The complaint alleged that Zuccarini would "redirect unsuspecting consumers to his Web sites and then trap them in a barrage of Web pages and pop-up browser windows."[93] It noted that he registered 15 misspellings of the domain name cartoonnetwork.com, misspellings of

powerpuffgirls.com, harrypotter.com and others,[94] domain names which were associated with web pages that contained no content. Rather, "[they] [we]re simply blank 'bridge' pages that instantaneously and invisibly redirect[ed] consumers to [Zuccarini's] commercial Web sites, which display[ed] advertisements for various goods and services, including online gambling and casinos, sweepstakes, lotteries, psychics, instant credit, or pornography."[95]

> "Typosquatting has become very tough to prosecute both internationally and domestically."

The *Zuccarini* court applied the three-factor test needed to succeed in an ACPA claim–first, whether the mark was famous or distinctive at the time of registration, secondly, whether the domain name is "identical or confusingly similar to" the mark, and thirdly, whether the domain-name registrant acted in bad faith.[96] In finding against Zuccarini,[97] the court found that all three factors had been met and that Zuccarini's typosquatting violated the federal cybersquatting law.[98]

In May 2002, the FTC won a permanent injunction against Zuccarini, barring him from obstructing a visitor's exit from a website.[99] However, he not only continued to use mousetrapping techniques on his current domain names, but continued to register new domain names as well.[100] At the time he was indicted in September 2003, most of his websites continued to delay or confuse a user's attempts to exit, and most still provided extensive sexually explicit content.[101]

IV. Typosquatting in the Criminal Arena: The Truth in Domain Names Act

A. Overview

Recently, a whole group of domain names have been affected by typosquatters: domain names that children are most likely to visit. Typosquatting has become very tough to prosecute both internationally and domestically. Unfortunately, the typosquatted websites did not merely lead children to competitors' websites; rather, they were leading them to obscene material and adult-oriented websites. This had a particularly devastating effect, since "Internet newbies get flustered and don't know how to get out of the site. Worse, children trapped inside a porn site may be frightened, both because of the site's content and a fear of being punished."[102]

Realizing the urgency of this problem, Congress swifty acted against typosquatters. The Truth in Domain Names Act was introduced to Congress on February 26, 2003.[103] Congressman Mike Pence (R-IN) sponsored it to punish those who use misleading domain names to attract children to sexually explicit sites.[104] According to Pence, the Act is "all about protecting the innocent from those who would prey upon them."[105] In advocating the bill, Pence referenced the Bible, saying "whoever causes one of the least of these (children) to sin ought to have a millstone tied around his neck. While we cannot legislate that retribution...we can pass the [Act]."[106]

The Truth in Domain Names Act became law on April 30, 2003.[107] It states that "[w]hoever knowingly uses a misleading domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity shall be fined...or imprisoned not more than two years, or both."[108] The law also calls for imprisonment of up to four years for the intent to deceive a minor into viewing material that is harmful to minors.[109] This marked the first time that any form of

cybersquatting could result in a felony conviction.[110]

B. *U.S. v. Zuccarini*

The first case under the Truth In Domain Names Act was brought against John Zuccarini, who was arrested on September, 3, 2003 in Hollywood, Florida. Prior to his arrest, Zuccarini, still playing games with trademark owners, had been the target of multiple civil suits. He moved to Nassau in an effort to evade trademark owners and the U.S. government. He used a registrar located in Germany for his domain registration activities. Whenever a decision went against him, he would file an appeal in German courts, which entered an injunction from the website being shut down and increased the costs of litigation for the plaintiffs. One civil case brought by the FTC involved Zuccarini registering domain names, 22 of which included the word "cupcake," which linked to pornographic or lewd websites.[111] According to the complaint, users would "have to click through as many as 30 separate windows or shut off the computer in order to escape from these pornographic pages."[112]
The government was receiving complaints about many of Zuccarini's websites, which redirected visitors to sexually explicit content. The most alarming aspect of these complaints was the fact that many of the websites were misspellings of popular children's websites, such as "bobthebuilder.com" or "disney.com." Unfortunately for the government, many of the websites that could lead to jail time for Zuccarini under the Act were created before the Act's passage. Therefore, the court would first have to find that the Act applied retroactively for Zuccarini. However, Zuccarini eventually pled guilty to 49 counts of using misleading domain names on December 10, 2003.[113] In addition, he pled guilty to one count of possessing child pornography.[114] He was sentenced on February 20, 2004, to 30 months in federal prison.[115] Congressman Pence commented, "[t]his conviction is one more step in making the Internet safe for our children."[116] He went on to say that "[c]reating misleading domain names is a way criminals used to get around the law and make money off of innocent children...this conviction puts scammers on notice that not only will their actions no longer be tolerated, but they will be prosecuted with the full force of the law."[117]

V. Is the TDNA an Unconstitutional Ban on Free Speech?

While nobody would doubt Congressman Pence's goals in passing the TDNA, a recent Supreme Court holding could nonetheless invalidate the statute. In *Ashcroft v. American Civil Liberties Union*, the Supreme Court noted that a statute which "effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another...is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[118] In *Ashcroft*, the Supreme Court reviewed the Child Online Protection Act[119] (COPA), a statute designed to protect minors from exposure to sexually explicit materials on the Internet.[120] Among other things, COPA imposed a $50,000 fine and six months in prison for knowingly posting, for "commercial purposes," content that is "harmful to minors" on the World Wide Web.[121] The statute, however, provided an affirmative defense

"Among other things, COPA imposed a $50,000 fine and six months in prison for knowingly posting, for "commercial purposes," content that is "harmful to minors" on the World Wide Web."

to those commercial Web speakers who restrict access to prohibited materials by "requiring the use of a credit card" or "any other reasonable measures that are feasible under available technology."[122] In affirming the Third Circuit's ruling, a divided Court found that enforcement of COPA should be enjoined because the statute likely violates the First Amendment; it remanded the case to the District Court for further proceedings on the issue.[123]

COPA, like the TDNA, was designed to protect children from accessing pornography on the Internet. The major difference between these two statutes is that COPA applies to all pornographic websites, [124] whereas the TDNA only applies to those that use misleading domain names.[125] Clearly this means that those convicted under the TDNA could cite *Ashcroft* in saying that TDNA is also likely an unconstitutional ban on free speech. A plaintiff could argue that, per *Ashcroft*, filtering software is a more effective alternative to an outright ban on misleading websites.[126] Furthermore, "the burden is on the Government to prove that the proposed alternatives will not be as effective as the challenged statute."[127] This test attempts to ensure "that speech is restricted no further than necessary to achieve the goal, for it is important to assure that legitimate speech is not chilled or punished."[128] In assessing claims, a court "should ask whether the challenged regulation is the least restrictive means among available, effective alternatives."[129]

While COPA and TDNA have their similarities, the Court would likely be able to find the TDNA constitutional, even if the statute were subject to strict scrutiny review. Unlike the affected websites in COPA, TDNA's websites are misleading by nature.[130] Typosquatted websites are considered illegal infringement on trademarked companies. An obscene website which does not infringe in any way is generally considered protected speech. However, by nature, typosquatted websites would likely lose this initial protection because they are not related to "legitimate" speech as required under the Court's test.[131] Therefore, typosquatted websites are probably not constitutionally protected.

If, however, a plaintiff can prove that the typosquatted websites are protected forms of free speech, the government will face an uphill battle to prove that an outright ban on the websites is the least effective alternative. Filtering technology may be at least as successful as a TDNA ban in restricting minors' access to harmful material online.[132] Filters also would not impose the burden on constitutionally protected speech that the TDNA imposes on adult users or Web site operators.[133] "Under a filtering regime, adults without children may gain access to speech they have a right to see ... [a]bove all, promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished."[134] In addition, "a filter can prevent minors from seeing all pornography, not just pornography posted to the Web from America... 40% of harmful-to-minors content comes from overseas."[135] However, "[f]iltering software, of course, is not a perfect solution to the problem of children gaining access to harmful-to-minors materials. It may block some materials that are not harmful to minors and fail to catch some that are."[136]

The government, however, can still make a solid argument against filtering software. Since typosquatted websites are generally illegal, a filter is probably not a true substitute for the TDNA. When Congress created the TDNA, it did not merely want to block these typosqutted websites from the eyes of children; it wanted to ban them altogether. Filtering software may help keep children from seeing most of the websites, but unlike the TDNA, it would not punish their creators. Deterrence was a critically important goal to Congress, and unless filtering software was used in tandem with the TDNA, that goal would probably not be achieved. If these goals are not met, filtering software could not be considered an adequate substitute to the TDNA.

VI. Is Criminal Liability Appropriate? If So, What Culpability Level Should Be Used?

In addition to finding that COPA was a likely violation of free speech, Justice Stevens' concurrence in *Ashcroft* questioned whether criminal sanctions are appropriate in cases involving obscenity.[137] Stevens noted that, "[c]riminal prosecutions are... an inappropriate means to regulate the universe of materials classified as 'obscene,' since 'the line between communications which "offend" and those which do not is too blurred to identify criminal conduct.'"[138] He continued, "Attaching criminal sanctions to a mistaken judgment about the contours of the novel

and nebulous category of 'harmful to minors' speech clearly imposes a heavy burden on the exercise of First Amendment freedoms."[139] Stevens and his more liberal peers on the court would likely subject this statute to strict scrutiny. However, they will still probably find that criminal liability is appropriate.

In *Ashcroft*, the Supreme Court noted that the "opinion does not hold that Congress is incapable of enacting any regulation of the Internet designed to prevent minors from gaining access to harmful materials."[140] Unlike COPA, the TDNA prohibits someone who "knowingly uses a *misleading* domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity..."[141] Congress is not trying to ban the material solely because it is obscene, but because it defames the goodwill of trademarked corporations and lures children to pornography. COPA applies to websites where children could find obscene material, but it does not apply to websites which children frequently visit. In addition, the Court would probably not find the material that Zuccarini was posting to be nebulous in nature. Zuccarini had the intent of steering children from legitimate, child-oriented websites to pornography solely for profit. This intent alone should subject him to criminal prosecution.

"Congress is not trying to ban the material solely because it is obscene, but because it defames the goodwill of trademarked corporations and lures children to pornography."

Is "knowingly" the appropriate culpability level for the TDNA? There are four *mens rea* culpability standards commonly used in the Model Penal Code.[142] These are (1) negligently, (2) recklessly, (3) knowingly, and (4) purposely.[143] Congress appropriately set the TDNA culpability standard at a higher level than negligent conduct.[144] "[Negligence] is distinguished from purposeful, knowing or reckless action in that it does not involve a state of awareness. A person acts negligently under this subsection when he *inadvertently* creates a substantial and unjustifiable risk of which he ought to be aware...a gross deviation from the care that would be exercised by a reasonable person in his situation."[145] To the contrary, typosquatting, as a violation of the TDNA, requires conscious decisions by the violator. The TDNA is not trying to catch Internet users like Mike Rowe,[146] who happened to register websites which are similar in name to trademarked companies. Under the TDNA, the violator must have the "intent to deceive a person into viewing obscenity."[147] Furthermore, the TDNA specifically notes that "a domain name that includes a word or words to indicate the sexual content of the site, such as 'sex' or 'porn,' is not misleading."[148]

Recklessness would also be an inappropriately low culpability standard in enforcing the TDNA. "[Recklessness] resembles acting knowingly in that a state of awareness is involved, but the awareness is of risk that is of a probability less than substantial certainty; the matter is contingent from the actor's point of view."[149] Typosquatting is an offense that should rarely lead to criminal liability. By nature, a typosquatter knowingly diverts traffic from one website to his own website through the mistakes of Internet users. As such, it seems inequitable for typosquatters to face criminal liability when they are not substantially certain that their website will lead to that response.

Given the rare circumstances under which typosquatters should face criminal sanctions, it seems that little harm could be done by raising the level from "knowingly" to "purposely." In the Model Penal Code, a narrow distinction is drawn between the two culpability levels. Knowledge that the requisite external circumstances exist is a common element in both conceptions.[150] But action is not purposive with respect to the nature or result of the actor's conduct unless it was his conscious object to perform an action of that nature or to cause such a result.[151] In other words, "[I]t is meaningful to think

of the actor's attitude as different if he is simply aware that his conduct is of the required nature or that the prohibited result is practically certain to follow from his conduct."[152]

While this distinction seems somewhat trivial, its application could foster divergent results when sentencing defendants. Leading minors to obscenity under the TDNA shifts the maximum penalty from two to four years.[153] A court could easily determine that the defendant in *U.S. v. Zuccarini* was purposely leading children to obscenity since he registered domain names for cartoons popular with children and typos of Disneyland.com. However, it is unlikely that future cases prosecuted under the TDNA will be so simple.

For instance, consider the example used above where a typosquatter registers the domain name mircosoft.com, and then connects it to obscene material. Microsoft.com's website receives approximately 190 million hits per day through 1.3 million visitors.[154] Clearly the typosquatter's domain name will receive heavy traffic, some of whom are likely to be minors. Moreover, it is likely that a larger percentage of younger minors will mistype the domain name they are searching for than adults. Should the court consider the defendant's actions as having the intent to deceive minors? This should be a question of fact for the jury to decide. However, even if the defendant knew that minors would visit the website in the example, he may not be certain that minors will visit the website. Should he, however, be subject to the higher penalty in this scenario? It seems unfair that the defendant be subject to the stiffer sentence if he knew that this was a possibility, but, unlike Zuccarini, this was not his purpose in registering the domain name. Even if a defendant is not liable under the proposed "purposely" standard, he would still be found guilty under subsection (a) of the statute and subject to two years in prison. Therefore, a change from "knowingly" to "purposely" under § 2252B(b) would better serve Congress' intentions.

> "If your domain name is likely to be reached by children, do not put links to obscenity on it, or you could be jailed as a felon."

VII. The Future of Typosquatting and the Effect of *U.S. v. Zuccarini*

Although case law on the subject is still in its infancy, Zuccarini was the perfect target for the Department of Justice to indict. It is no coincidence that the flagship case under the ACPA and the initial case filed under the TDNA were filed against Zuccarini. The FTC had been on his tail since 1999 and had shut down over 200 websites that he owned.[155] By setting an example against one of the biggest squatters in the Internet's history, the Department hopes to broadcast Congressman Pence's message to all those who squat on domain names: if your domain name is likely to be reached by children, do not put links to obscenity on it, or you could be jailed as a felon.

While any parent would argue against the lenient treatment for someone who registers a website with the sole intent of leading children to pornography or other forms of obscenity, major questions regarding the law's effectiveness have yet to be answered by the court. Until the law has actually been tested in the judicial system through a full trial, new domain names that lure children to pornography could still appear.

The vast majority of the websites registered in Zuccarini's case had been registered before the enactment of the new law. Because the TDNA does not explicitly state that it applies retroactively, Zuccarini forewent arguing that, while he may be subject to civil liability under the ACPA, he did not violate the TDNA with any website registered prior to April 2003. However, after the legislation was

enacted, Zuccarini failed to take notice and remove the offending websites. Since, at the time of his indictment, he had multiple websites targeting children to pornography that were created after TDNA's enactment, he was unable to escape liability through this defense. However, future defendants could have this defense available to them if they registered the domain names prior to April of 2003.

However, the Department of Justice would likely win the retroactivity argument by citing *Ford Motor Co. v. Catalanotte*.[156] In *Catalanotte*, the registrant, an employee of the plaintiff motor company, registered an Internet domain name that included the name of the motor company's employee newspaper.[157] Almost four years later, the registrant sent an email to officers of the motor company falsely stating that he had received offers for the domain name and extended an offer to the company to acquire the name.[158] The court affirmed the judgment in favor of the company, rejecting the registrant's contention that the ACPA precluded liability based on domain names that were registered prior to enactment of the ACPA.[159] The court found that, under the plain language of the ACPA, liability could be based on trafficking that occurred after the ACPA's enactment regardless of when the domain name was registered.[160] The court also concluded that the registrant "trafficked" in the domain name for the purposes of the ACPA when he offered it for sale to the company.[161]

Since the passage of the TDNA, Internet users can expect a steady reduction in the number of typosquatted websites which lead to obscenity. The Department of Justice made it clear that it would not tolerate common misspellings of popular children's websites. For instance, "dinseyland.com", a website created by Zuccarini and a misspelling of "disneyland.com," was eventually shut down.

The outcome of the FTC's case against Zuccarini will potentially have huge impacts on criminal and civil cyber law cases across the globe. If Zuccarini serves jail time, the FTC will send a clear message to cybersquatters across the country through the TDNA that it will not tolerate cyber crimes involving obscenity. Moreover, the 30 month sentence will provide a strong deterrent against those predators who lure children to pornographic websites in the name of money and could virtually wipe clean all U.S. based domain names that do so.

A. Should all Typosquatting be Criminalized?

The vast majority of typosquatters do not register websites that a child could accidentally misspell. Consequently, only a small niche of typosquatters will likely be deterred by the TDNA. Unfortunately, typosquatting as a whole will probably not be reduced until more steps can be taken. Squatters are continuing to find profitable ways to register domain names. For instance, in response to the Third Circuit's ruling that mousetrapping is illegal under the ACPA, typosquatters could begin to offer products similar to the trademarked site. Typosquatters will continue to push the boundaries set by Congress. Since all encompassing legislation against typosquatting could be years away, and changes through the judiciary are usually reactive instead of proactive, most squatters will still continue to register websites. More options are necessary so that trademark-bearing companies can resolve the issues they currently face.

Many typosquatters, however, do not redirect Internet users to pornography or other annoyances; rather, they are competitors looking to get an edge in the virtual marketplace. We live in an economy driven by capitalism. Competition in any industry will likely drive the price of the goods down and ultimately benefit the consumer. Companies in competition do not have the same utter disregard for the innocence of children as Zuccarini; they are, however, still motivated by the prospect of profit. Therefore, it does not seem fair that all typosquatted cases be adjudicated on criminal grounds.

B. Alternatives to Litigation

While cybersquatting violations are already noted, typosquatters differ from the general class of cybersquatters in that they register domain names after a trademark owner has already established a domain name using their trademark. Whether the typosquatter registers first is irrelevant in typosquatting cases, unlike cybersquatting cases, because typosquatters seek sites with high traffic. In addition, the TDNA is unlikely to have major effects on typosquatting outside of the United States, even if the validity of the statute is tested in court, unless other countries follow suit and enact similar laws. The cyberlaw of most other countries is less advanced than that of the United States. This is commonly affected due to the country's customs, legal systems, and economies. Because of this, laws similar to the TDNA are probably not in the

immediate future. Accordingly, preventing typosquatters from registering an alternative might be easier than finding a flawless cure for the damage done.

> "The complexities of resolving disputes over domain names and trademarks increases dramatically when a business decides to expand internationally."

i. Stopping the Problem Before it Develops: Registering Potential Misspellings

An obvious way for trademark holders to prevent typosquatting is to register as many misspellings of their domain name as possible. While registration does have its costs (about twenty dollars per domain name), the costs pale in comparison to the litigation costs and harm that could be done to their trademarks. This option is easiest for new businesses that are still in the process of registering their domain names and their trademarks. For mature companies, however, this may not be an option. Only 163 of the Fortune 500 companies actually own a majority of the registrations of their domain names.[162] This shows that mature companies are neither actively nor sufficiently policing their domain names. However, these businesses can still put up a fight through registration. One method of fighting typosquatting is through new software. In *The Economic Times*, Greg Kapan, a senior consultant for Ernst & Young recommends Linkscan 9.0, which can help people discover suspicious links.[163] As he explains, "[a]bout two [hundred thousand] names expire each month, either intentionally or accidentally. This software helps aggregators pick up domain names in bulk as soon as they expire."[164] Kapan further notes that "the U.S. Department of Education, which has over sixty-five thousand internal and external links, discovered through software that fifteen of these links were linked to porn sites."[165] Through this type of software, companies can easily trace and discover domain names that are being used by cybersquatters so they do not remain under their radar.

ii. A Universal Reporting System

A potential alternative to fight typosquatting is a universal method for corporations and Internet users to report and give notice to the FTC for typosquatting violations. Trademark holders should receive notice when someone attempts to register either their trademark or a common misspelling of it. The FTC receives thousands of complaints from consumers and businesses involving mousetrapping techniques by the squatters. However, without international jurisdiction, they are helpless to stop international incidents.

The complexities of resolving disputes over domain names and trademarks increases dramatically when a business decides to go international. Governments have a role in "manag[ing] or establish[ing] policy for their own [country code domain names]."[166] The trademarked businesses, on the other hand, have the resources and motivation to pursue the offenders in international courts. Thus, potential notification methods whereby complaints are given to trademark holders through either the FTC or the Patent and Trademark Office should be considered in the future.[167] Although the cost of such an option would be expensive at the beginning, it would provide notice to marked companies who have been the targets of typosquatters to determine how to tackle the problem.

iii. Parental Guidance and Controls

While these alternatives are both highly effective ways to reduce the chances of children seeing obscene material on the Internet, parents and guardians provide the best alternative. Easy suggestions include downloadable software, such as the Family Browser, which automatically blocks web browsers from reaching obscene websites. Such software is free and can be downloaded on

downloads.com. In addition, parents can put their computers in a central location in their house to better monitor their children's surfing habits. Alternatives like these are cheap, cost effective, and should be considered by any parent who has a child on the Internet.

VIII. Conclusion

Given the increasing popularity in pornographic websites and the Internet as a whole, it is unlikely that trademark holders will ever completely rid themselves of the problems created by typosquatting. However, because of society's great concern for its children, Congress has taken a giant leap forward in the fight against typosquatting.

In addition, TDNA is likely sufficiently different from COPA in that it would probably not be found unconstitutional. While the statute will not end the problem, Congress has sent a clear message through the TDNA and Zuccarini's conviction that it is possible to fight typosquatting, especially when it involves crimes against children. Furthermore, Congress has indicated that we can and will clean up the Internet to protect children. Typosquatters like Zuccarini will continue to change their methods and adapt to legislation, but progress can certainly minimize the effects of such efforts if parents, guardians, and trademark holders actively report such websites and monitor the Internet surfing habits of children.

Endnotes

* J.D. Candidate, 2005, Vanderbilt University School of Law.

[1] Robyn Greenspan, *Porn Pages Reach 260 Million, available at* http://www.esecurityplanet.com/trends/article.php/3083001 (Sept. 25, 2003).

[2] *Id.*

[3] *See* 18 U.S.C. § 1470 (2004).

[4] *Pornography Victim Protection: Hearing Before the Senate Judiciary Comm.*, 108th Cong. (2003) (Statement of John Malcolm, Deputy Assistant Attorney General, Criminal Division).

[5] Matt Pyeatt, *Teen Internet Porn Study Stirs Debate*, CNSNews.com, *available at* http://www.aclj.org/News/Pornography/011212_Teen_Porn_Study.Asp (Dec. 12, 2001) (emphasis added).

[6] For example, "www.whitehouse.com" is a website that many people would think is the official homepage for the White House, however it is a pornographic website (last visited Sept. 15, 2004) The actual White House website is www.whitehouse.gov. The owner of www.whitehouse.com recently put his domain name up for sale.

[7] Robert Cumbow possibly coined the term "typosquatter" and was one of the first to recognize this expanding sub-species of cybersquatters. Robert C. Cumbow, *"Typosquatters" Post Threat to Trademark Owners on the Web*, N.Y. L.J., Oct. 13, 1998, at S2.

[8] Jonathan M. Ward, *The Rise and Fall of Internet Fences: The Overbroad Protection of the Anticybersquatting Consumer Protection Act*, 5 MARQ. INTELL. PROP. L. REV. 211, 215 (2001) (quoting Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1233 (N.D. Ill. 1996)).

[9] *Id.*

[10] Benjamin Edelman, *Large-Scale Registration of Domains with Typographical Errors, at* http://cyber.law.harvard.edu/people/edelman/typo-domains/ (last modified Sept. 3, 2003).

[11] Dara Gilwit, *The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How To Prevent Public Deception and Trademark Infringement*, 11 WASH. U. J.L. & POL'Y 267, 268-269 (2003).

[12] *Id.* at 269.

[13] Typosquatters usually make a delineated profit each time someone stumbles into their website and they click on one of the advertisements on the banners or windows which pop up. *See* Edelman, *supra* note 10.

[14] John Zuccarini registered multiple misspellings of Nickelodeon, discussed further *infra*.

[15] 15 U.S.C. § 1129 (2004).

[16] *See generally* Gilwit, *supra* note 11.

[17] 18 U.S.C. § 2252B (2004).

[18] *See generally* 149 CONG. REC. H. 1363 (2003).

[19] *See* Heather Walmsley, *Laying down the law: are you a model online citizen or do you risk a confrontation with the sheriff by riding roughshod over your legal obligations? Judge for yourself with our guide to staying out of jail in this Web-horse town*, INTERNET MAGAZINE, Dec. 2003, at 48.

[20] *Id.*

[21] Edelman, *supra* note 10.

[22] Congressional Press Release, Pence Heralds First Conviction Under Truth in Domain Names Law He Authored

(Dec. 11, 2003), *available at* http://mikepence.house.gov/News/DocumentSingle.aspx?DocumentID=4926.

[23] *Id.*

[24] 124 S. Ct. 2783 (2004).

[25] Sung Yang, *Staking a Claim in Cyberspace: An Overview of Domain Name Disputes*, 36 WILLAMETTE L. REV. 115 (2000).

[26] *Id.*

[27] *Id.* at 116.

[28] *Id.*

[29] Rebecca W. Gole, *Playing the Name Game: A Glimpse at the Future of the Internet* ***Domain Name*** *System*, 51 FED. COMM. L.J. 403, 406 (1999).

[30] *See* Wayne Brooks, *Wrestling Over the World Wide Web: ICANN's Uniform Dispute Resolution Policy for Domain Name Disputes*, 22 HAMLINE J. PUB. L. & POL'Y 297, 304-05 (2001).

[31] *Id.*

[32] *Id.*

[33] BLACK'S LAW DICTIONARY 1530 (8th ed. 2004).

[34] Zohar Efroni, *The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: New Opportunities For International Forum Shopping?*, 26 COLUM. J.L. & ARTS 335, 336 (2003).

[35] Brooks, *supra* note 30, at 305.

[36] *Id.*

[37] Efroni, *supra* note 33, at 336-37.

[38] *Id.* at 337.

[39] *Id.* at 337-38.

[40] *Id.* at 336-37.

[41] *Id.* at 337.

[42] *Id.*

[43] Gilwit, *supra* note 11, at 273.

[44] *Id.*

[45] *Id.*

[46] H.R. REP. NO. 106-412, at 8 (1999).

[47] Gilwit, *supra* note 11, at 274 (citing Brookfield Communications, Inc. v. West Coast Entm't Corp., 174 F.3d 1036, 1044 (9th Cir. 1999).

[48] *Id.* at 272; *see also* https://www.domainregistry.com/register/ for a typical domain name registration form (illustrating that the only materials required for registration are a name, address, e-mail address, phone number, and the $30 registration fee) (Last Visited Sept. 15, 2004).

[49] Gilwit, *supra* note 11, at 274.

[50] *Id.* at 274-75.

[51] *See* 15 U.S.C. § 1125 (2004).

[52] *See generally* Gilwit, *supra* note 11.

[53] *See* Gilwit, *supra* note 11, at 275.

[54] *See generally* Edelman, *supra* note 10.

[55] 15 U.S.C. §§ 1051-1127 (Supp. 2001).

[56] *Id.* § 1125(c).

[57] Gilwit, *supra* note 11, at 276 (citing Donna Frazier Schmitt, Intellectual Property and Technology 1 (2001) (unpublished course material for Entertainment Planning & Drafting at Washington University School of Law, on file with the Washington University Journal of Law & Policy) (noting: "Before bringing an action, a trademark owner may send a "Cease and Desist" letter to the owner of a cite to alert them of the claimed infringement. Because most infringers are not aware of the consequences for using another's trademark, this letter gives them the opportunity to comply or be forced into legal action. If a trademark owner sends a cease and desist letter, it must be done after a thorough investigation. Moreover, a trademark owner must recognize the possibility that a party may respond by filing an action for Declaratory Judgment.")).

[58] Erika M. Brown, The Extraterritorial Reach of United States Trademark Law: A Recent Review of Discussions under the Lanham Act, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 863, 863.

[59] Gilwit, *supra* note 11, at 276.

[60] *Id.* at 277.

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *See* Brookfield Communications, Inc. v. West Coast Entertainment Corp, 174 F.3d 1036, 1053-54 (9th Cir. 1999) (Generally, a plaintiff must demonstrate a likelihood of confusion by establishing that the public believes the mark's

owner authorized the use of the trademark. To assess the consumer's "likelihood of confusion" in the marketplace, the court employs the following factors: (1) strength of the plaintiff's mark; (2) relatedness of the services; (3) similarity of the marks; (4) evidence of actual confusion; (5) marketing channels used; (6) likely degree of purchaser care and sophistication; (7) intent of the defendant in selecting the mark; and (8) likelihood of expansion of the product lines using the marks.) (holding that Internet users might confuse plaintiff's database with defendant's website because of the similarities between plaintiff's "Movie Buff" movie database software and defendant's online movie sales website at "moviebuff.com").

[65] Ward, *supra* note 8, at 219.

[66] Gilwit, *supra* note 11, at 278.

[67] *Id.*

[68] Jason M. Osborn, Note, *Effective and Complimentary Solutions to Domain Name Disputes: ICANN's Uniform Domain Name Dispute Resolution Policy and the Federal Anticybersquatting Consumer Protection Act of 1999*, 76 NOTRE DAME L. REV. 209 at 220 (Nov. 2000).

[69] Jessica Lee, *Bill Would Protect Trademarks, Names from Cybersquatters*, USA TODAY, Aug. 3, 1999, at 8A.

[70] Yang, *supra* note 25, at 136.

[71] *Id.* at 137.

[72] 15 U.S.C. § 1129 (2004); ICANN, Uniform Domain Name Dispute Resolution Policy, *available at* http://www.icann.org/dndr/udrp/policy.htm (Oct. 24, 1999) [hereinafter ICANN Policy].

[73] Gilwit, *supra* note 11, at 280 (quoting S. REP. NO. 106-140, at 4 (1999)).

[74] 15 U.S.C. §1125(d) (2004).

[75] *See Generally* 15 USC §1125 (2004). This statute also imposes a balancing test to be used by courts in determining liability and guilt.

[76] *Id.*

[77] *See* Bochan v. La Fontaine, 68 F. Supp 2d 692, 702 (E.D. Va. 1999), for recent case law on the issue; Gole, *supra*, note 29, for a discussion of the "effect doctrine" and how it affects this issue. *See generally* Donna L. Howard, *Trademarks and Service Marks and Internet Domain Names: Giving ICANN Deference*, 33 ARIZ. ST. L.J. 637, 650 (2001), for a more thorough discussion of the personal jurisdiction issue as it relates to cybersquatting.

[78] *See* Brooks, *supra* note 30, 316 (citing Luke A. Walker, *Intellectual Property; Trademark, ICANN's Uniform Domain Name Dispute Resolution Policy*, 15 BERKELEY TECH. L.J. 289, 300 (2000)).

[79] *Id.*; *see also* ICANN Policy, *supra* note 72.

[80] *See* Edelman, *supra* note 10.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] The Registrar's Whois database contains records of the names and addresses of the owners of each domain name registered with that particular registrar. *See generally* http://www.internetprivacyadvocate.org/ProtectYourPersonalInfo.htm for more information regarding Whois databases (last visited Sept. 15, 2004).

[85] *See* Edelman, *supra* note 10.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] Shields v. Zuccarini, 254 F.3d 476, 487 (3rd Cir. 2001).

[90] *Id.* at 479.

[91] *Id.* at 480.

[92] *Shields*, 254 F.3d at 480.

[93] FTC v. John Zuccarini, Compl. pg. 5, on file with author.

[94] *Id.* at 6.

[95] *Id.* at 7.

[96] *Id.*

[97] See *Shields*, 254 F.3d at 486-88, (noting that the court held in favor of Shields, the plaintiff, awarding him $10,000 per offending website, his attorney's fees and an injunction. The ACPA provides for statutory damages if a party violates 1125(d)(1) "in the amount of not less than $ 1,000 and not more than $ 100,000 per domain name, as the court considers just." *Id.* at 486 (quoting 15 U.S.C. § 1117(d) (2000)). Additionally, the ACPA provides that "the court in exceptional cases may award reasonable attorney fees to the prevailing party." *Id.* at 487 (quoting 15 U.S.C. § 1117(a)). In traditional trademark infringement cases, a court must find that the losing party had "culpable conduct ... such as bad faith, fraud, malice or knowing infringement before a case qualifies as 'exceptional'." *Id.* The court found that Zuccarini acted willfully and in bad faith when he, with the intention of confusing people and diverting Internet traffic to his own websites for financial profit, registered the "Joe

Cartoon" domain name. *Id.* at 487. Thus, the court held that Zuccarini's actions, coupled with his "lack of contrition," constituted an "exceptional" case, entitling Shields to his attorney's fees. *Id.* at 486-87. Additionally, the court issued a permanent injunction against Zuccarini. *Id.* at 486. The court held that because a finding of likelihood of confusion meant a finding of irreparable injury, Shields was entitled to a permanent injunction. *Id.* Shields would "suffer damage to his reputation and a loss of goodwill if Zuccarini is allowed to operate his offending web sites." *Id.* Largely, Shields' livelihood and fame depended on Internet users' ability to access his sites without being trapped in Zuccarini's sites or barraged by images displayed therein, which users may attribute to him. *Id.* Thus, without the permanent injunction, Shields would be irreparably harmed. *Id.* Moreover, because Zuccarini has more than three thousand of these websites, his harm from the financial loss of the five websites would be miniscule. *Id.* The court further noted that "public interest ... is a synonym for the right of the public not to be deceived or confused." *Id.* (quoting Opticians Ass'n. of Am. v. Independent Opticians of Am., 920 F.2d 187, 197 (3d Cir. 1990)). Consequently, the injunction was in the public's best interest. *Id.*).

[98] *Id.* at 487.

[99] *See* FTC v. Zuccarini, No. 01-CV-4854 2002 U.S. Dist. LEXIS 13324, at *12 (E.D. Pa. 2002).

[100] *See* Edelman, *supra* note 10.

[101] *See generally*, Complaint, United States v. Zuccarini, (S.D.N.Y. 2003), *available at* http://news.findlaw.com/cnn/docs/cyberlaw/uszuccarini82903cmp.pdf.

[102] *See* Ruma Singh, *It's Easy to Stumble on to Porn on the Net*, THE ECONOMIC TIMES OF INDIA, Feb. 15, 2004. (quoting Connie Eccles, CEO of ComPortOne).

[103] 149 CONG. REC. H. 1363 (2003) (statement of Rep. Pence).

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] 18 U.S.C. § 2252B(a) (2004).

[109] *Id.* § 2252B(b).

[110] *See* Walmsley, *supra* note 19.

[111] *See* Complaint, *supra* note 94, at 5.

[112] *Id.*

[113] *See* Walmsley, *supra* note 19.

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] Ashcroft v. ACLU, 1245 S. Ct. 2783, 2791 (2004) (quoting Reno v. ACLU, 521 U.S. 844, 874 (1997)).

[119] 47 U.S.C. § 231 (2002).

[120] *See generally*, *Ashcroft*, 1245 S. Ct. at 2783.

[121] 47 U.S.C. § 231(a)(1).

[122] *Id.* § 231(c)(1).

[123] *Ashcroft*, 124 S. Ct. at 2783.

[124] 47 U.S.C. § 231(a)(1).

[125] 18 U.S.C. § 2252B(a) (2004).

[126] *Ashcroft*, 124 S. Ct. at 2795.

[127] *Id.* at 2791 (citing *Reno*, 521 U.S. 844, 874 (1997)).

[128] *Id.*

[129] *Id.*

[130] 18 U.S.C. § 2252B(a).

[131] *Ashcroft*, 124 S. Ct. at 2791 (noting that the purpose of the "least restrictive alternative" approach is to assure that legitimate speech is not punished).

[132] Adapting the *Ashcroft* Court's reasoning regarding COPA to a parallel use with TDNA. *Ashcroft*, 124 S. Ct. at 2790.

[133] *Id.*

[134] *Ashcroft*, 124 S. Ct. at 2792.

[135] *Id.*

[136] *Id.* at 2793; *see* ACLU v. Reno, 31 F. Supp. 2d 473, 492 (E.D. Pa. 1999) (noting that blocking and filtering software is not perfect, thus minors may still be able to access inappropriate material or be blocked from age-appropriate material).

[137] *Id.* at 2796. (Stevens, J., concurring).

[138] *Id.* (quoting Smith v. United States, 431 U.S. 291, 316 (1977) (Stevens, J., dissenting)).

[139] *Ashcroft*, 124 S. Ct. at 2796 (Stevens, J., concurring).

[140] *Id.* at 2795.

[141] 18 U.S.C. § 2252B(a) (2004).

[142] MODEL PENAL CODE § 2.02(2)(a)-(d) (1962) (While the TDNA is not codified under the Model Penal Code (MPC), the MPC's definitions of the culpability standards are typically applied in federal courts).

[143] *Id.* Negligence is the lowest defined standard under which the criminal "should be aware of a substantial and unjustifiable risk that the material element exists or will result from his conduct." MODEL PENAL CODE §2.02(2)(d). A person is reckless when he "consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. MODEL PENAL CODE § 2.02(2)(c). Knowledge, the minimum standard required under the TDNA, is present "if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist" and "he is aware that it is practically certain that his conduct will cause such a result." MODEL PENAL CODE § 2.02(2)(b)(i)-(ii). Purpose, the highest standard with respect to a material element of an offense, is present when, "...it is his conscious object to engage in conduct of that nature or to cause such a result" and "he is aware of the existence of such circumstances or he believes or hopes that they exist." MODEL PENAL CODE § 2.02(2)(a)(i)-(ii).

[144] 18 U.S.C. § 2252B(a) (making "knowledge" the culpability standard).

[145] SANFORD H. KADISH & STEPHEN J. SCHULHOFER, CRIMINAL LAW AND ITS PROCESSES 209 (emphasis added).

[146] Mike Rowe is a 17 year old student from Canada who registered the website "www.mikerowesoft.com" because his name was similar to the company Microsoft. Microsoft told him to either sell his website for the $10 he purchased it for or face litigation. For further information on this story, *see* Daniel Sleberg, *Teen Fights to Keep MikeRoweSoft.com*, CNN, Jan. 20, 2004, *available at* http://www.cnn.com/2004/TECH/internet/01/20/rowe.fight/index.html.

[147] 18 U.S.C. § 2252B(a).

[148] *Id.* § 2252B(c).

[149] *See* KADISH, *supra* note 147, at 210.

[150] *Id.*

[151] *Id.*

[152] *Id.* at 209.

[153] 18 U.S.C. § 2252B(b) (2004).

[154] *Extra! Read All About Us!*, Microsoft, *at* http://www.microsoft.com/misc/features/features_extra.htm (last visited Sept. 15, 2004).

[155] *Cybersquatter Accused of Luring Children to Porn Sites*, 5 No. 2 ANDREWS E-BUS. L. BULL. 4 (2003).

[156] Ford Motor Co. v. Catalanotte, 342 F.3d 543 (6th Cir. 2003).

[157] *Id.* at 545.

[158] *Id.*

[159] *Id.* at 547.

[160] *Id.* at 548.

[161] *Id.* at 549.

[162] Craig A. Pintens, Comment, *Managing the "Team" on the Field, Off the Field, and in Cyberspace: Preventing Cybersquatters from Hijacking Your Franchise's Domain Names*, 11 MARQ. SPORTS L. REV. 299, 324 (2001) (quoting *Majority of Fortune 500 Have More of Their Domain Names Pirated Than They Actually Own*, BUS. WIRE, Mar. 2, 2000, at 1).

[163] *See* Walmsley, *supra* note 19.

[164] *Id.*

[165] *Id.*

[166] Management of Internet Names and Addresses, 63 Fed. Reg. 31741 (June 10, 1998).

[167] *See* Gilwit, *supra* note 11, at 292-94. In her extensive proposal, Dara Gilwit discusses the effectiveness of a notice system, proposing a system where the new service determines whether the domain name registrant is using the domain name with a bad-faith intent, whether the domain name is likely to confuse consumers, and whether hit is being used commercially. She concludes that although costlier upfront, it would avoid the expenses of court action or arbitration, thereby saving money in the long run.

film & tv