

2010

The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites

Thomas J. Curtin

Follow this and additional works at: <http://brooklynworks.brooklaw.edu/jlp>

Recommended Citation

Thomas J. Curtin, *The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites*, 19 J. L. & Pol'y (2010).
Available at: <http://brooklynworks.brooklaw.edu/jlp/vol19/iss1/13>

This Note is brought to you for free and open access by BrooklynWorks. It has been accepted for inclusion in Journal of Law and Policy by an authorized administrator of BrooklynWorks. For more information, please contact matilda.garrido@brooklaw.edu.

THE NAME GAME: CYBERSQUATTING AND TRADEMARK INFRINGEMENT ON SOCIAL MEDIA WEBSITES

*Thomas J. Curtin**

INTRODUCTION

Over the past decade, Internet use has grown astronomically,¹ allowing Internet users to have increased control over web page creation, and permitting Internet users to create unique profiles for social networking.² With such growth and evolution, the Internet has also become a dangerous venue where individuals hijack domain names and profit off the damage caused to a brand name. For example, were an Internet user to accidentally type “Citybank.org,” instead of “Citibank.org,” into his browser to perform online banking activities, he would stumble upon a website with misleading Citibank advertisements that would

* J.D. Candidate, Brooklyn Law School, 2011; B.A., Fordham University, 2008. I would like to thank my friends and family for their support during the writing process. I would also like to thank Professor Bambauer for his guidance on this topic.

¹ See *Internet Growth Statistics*, INTERNET WORLD STATS, <http://www.internetworldstats.com/emarketing.htm> (last updated July 30, 2010) (showing that in 1995, only 16 million users browsed the Internet, while in 2010, that number skyrocketed to 1.65 billion users).

² See Maria Markella, *The Web 2.0 Phenomenon: Another Trend?*, BUZZLE.COM, <http://www.buzzle.com/articles/web-20-phenomenon-another-internet-trend.html> (noting that the movement is characterized by websites, such as Myspace, which allow “users to take active part in the development of a webpage’s content and history”); see also Tim O’Reilly, *What is Web 2.0*, O’REILLY MEDIA (Sept. 30, 2005), <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1> (discussing how the burst of the dot com bubble in the earlier part of the decade gave rise to a phenomenon known as Web 2.0, which makes software much more accessible to browsers).

redirect him to competitors' websites.³ The resulting frustration in being redirected to the wrong website would be directed in part toward Citibank and its goodwill.⁴ Such diversions, as in the Citigroup example, are not accidents; rather, they are scams intended to bring Internet users to competitors' sites so that the domain name owners make a profit off of the Internet user's mistake.

This process, known as cybersquatting, is a form of trademark infringement.⁵ Cybersquatting involves the bad faith registration of "well-known brand names as Internet domain names in order to force the rightful owners of the marks to pay for the right to engage in electronic commerce under [their own trademark]."⁶ Cybersquatters hurry to a domain registration site to register a domain name similar to another company's trademark before that company has had the chance to protect and fully use its trademark.⁷ To cite one example, an impostor registered the domain name "attphonecard.com" and established a website that solicited credit card information from Internet users.⁸ In this case, the Internet user wonders why he stumbled on an unrelated website, which he did not intend to visit, and which then fraudulently obtained his financial information. The abusive registration of this domain name harmed the AT&T brand and the consumer's frustration resulting from this scam likely was directed at AT&T and its mark.⁹ Such abusive registration of domain names confuses the consumer and allows the infringer to profit off of his misconduct.¹⁰

³ Citigroup, Inc. v. Chen Bao Shui, 611 F. Supp. 2d 507, 511 (E.D. Va. 2009).

⁴ See *id.* Indeed, the court in *Citigroup* noted that the defendant reserved this domain name solely to garner click through revenue. *Id.*

⁵ See *Virtual Works Inc. v. Volkswagen of Am., Inc.*, 238 F.3d 264, 267 (4th Cir. 2001) (describing how cybersquatting is the "Internet version of a land grab").

⁶ *Id.* (citing S. REP. NO. 106-140, at 4 (1999)).

⁷ *Id.* at 267.

⁸ *Cybersquatting and Consumer Protection: Ensuring Domain Name Integrity: Hearing on S. 1255 Before the Comm. on the Judiciary*, S. REP. NO. 106-140, 106th Cong. 8 (1999) (statement of Anne H. Chasser, President, Int'l Trademark Ass'n).

⁹ See *id.*

¹⁰ *Hamptons Locations, Inc. v. Rubens*, 640 F. Supp. 2d 208, 218

Trademark infringement on the Internet is not merely confined to squatting on a domain name; courts have also held that trademark infringement includes abusively reserving “metatags”¹¹ similar to famous brands on search engines such as Google.¹² In this form of infringement, the impostor¹³ uses famous brand names as hidden text in the website, which, in turn, creates search words on search engines to lead the consumer to an impostor website.¹⁴ These metatags are a form of infringement because, if used in an abusive manner, they act as a mechanism to traffic Internet users to an impostor website.¹⁵

On June 13, 2009, Facebook,¹⁶ a social media site boasting 500 million active members,¹⁷ unveiled a new username feature that allowed its users to create distinct web addresses, or “vanity

(E.D.N.Y. 2009).

¹¹ “Metatags are HTML code intended to describe the contents of the web site The more often a term appears in the metatags and in the text of the web page, the more likely it is that the web page will be “hit” in a search for that keyword and the higher on the list of “hits” the web page will appear.” *Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp.*, 174 F.3d 1036, 1045 (9th Cir. 1999).

¹² *See Promatek Indus. Ltd. v. Equitrac Corp.*, 300 F.3d 808, 815 (7th Cir. 2002) (“Consumers who are directed to Equitrac’s webpage [as a result of the infringing metatag] are likely to learn more about Equitrac and its products before beginning a new search for Promatek and Copitrac.”); *see generally* THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:69 (4th ed. 2010) (describing how the Lanham Act applies to metatags).

¹³ For the purposes of this Note, “impostor” will refer generally to cybersquatters.

¹⁴ *See, e.g., Aztar Corp. v. MGM Casino*, No. 00-833-A, 2001 WL 939070, at *5 (E.D. Va. 2001) (describing how defendant used Tropicana as a metatag to traffic browsers to his infringing website, “tropicanascasino.com”).

¹⁵ *Id.*; *Kraft Food Holdings, Inc. v. Helm*, 205 F. Supp. 2d 942, 944 (N.D. Ill. 2002) (noting how defendant used “VeVeeda” as a metatag to direct browsers to a pornographic website entitled “cheesygraphics.com”).

¹⁶ Facebook is the most popular social media website, and allows individuals to create profiles, add friends, and join networks organized by school, workplace, or location. Josie Myers, *What is Facebook?*, WISEGEEK, <http://www.wisegeek.com/what-is-facebook.htm> (last visited Sept. 13, 2010).

¹⁷ *Statistics*, FACEBOOK, <http://www.facebook.com/press/info.php?statistics> (last visited Sept. 13, 2010).

URLs,”¹⁸ for their profiles.¹⁹ On the one hand, the feature is beneficial in that it allows users to express themselves and makes it easier for other users to connect with them.²⁰ In addition, the vanity URL cuts search costs by allowing individuals to use their names and allowing companies to use their brands as usernames.²¹ On the other hand, the feature also makes it easier to hijack a trademark by allowing impostors to reserve a brand name as their usernames.

Before Facebook launched its username feature, users on other social media sites, such as Twitter²² and Myspace,²³ abused the username feature and reserved others’ names to pose as celebrities; users also created impostor profiles that maligned the celebrities’ character.²⁴ For example, on Twitter, impostors posed as well-

¹⁸ The username functions as a “vanity URL” because the reservation of the username changes the URL from a numerical identification number to the individual’s or corporation’s name. See Peter T. Wakiyama & Odia Kagan, *Facebook Vanity URLs May Hurt More Than Just One’s Pride*, 21 NO. 9. INTELL. PROP. & TECH. L.J. 7 (2009) (“On June 13, 2009, Facebook vanity URLs opened for registration by its users. Instead of www.facebook.com/id=591932074, a user’s page would now be located at www.facebook.com/johndoe, allowing the user to be easily found by entering his or her name into the URL in the browser.”).

¹⁹ See Blaise DiPersia, *Coming Soon: Facebook Usernames*, THE FACEBOOK BLOG (June 9, 2009, 12:11PM), <http://blog.facebook.com/blog.php?post=90316352130> (highlighting the usefulness of the Facebook username feature).

²⁰ *Id.*

²¹ *See id.*

²² Twitter is a social media website that enables users to post thoughts and messages as “tweets,” and allows individuals to follow others’ tweets. *About Twitter*, TWITTER, <http://twitter.com/about> (last visited Sept. 13, 2010). Additionally, the website allows individuals to group tweets together using “hashtags,” which appears in search engine results, including on Twitter’s home page. TECH FOR LUDDITES (Feb. 18, 2009), <http://www.techforluddites.com/2009/02/the-twitter-hash-tag-what-is-it-and-how-do-you-use-it.html>.

²³ MySpace enables individuals to create unique profiles, add friends, and send messages, thereby empowering “its global community to experience the Internet through a social lens by integrating personal profiles, photos, videos, mobile, messaging, games, and the world’s largest music community.” *MySpace Press Room*, MYSPACE, <http://www.myspace.com/pressroom> (last visited Sept. 13, 2010).

²⁴ See Douglas MacMillan, *LaRussa v. Twitter Tests Web Anonymity*,

known figures such as the Dalai Lama and Kanye West.²⁵ Needless to say, celebrities were not pleased with these impersonations.²⁶ In one recent illustration of this problem, an anonymous user created an impostor account for BP, titled “BPGlobalPR,” mocking the company for its handling of the oil spill.²⁷ The mock account was followed by almost 145,000 people, and the fake profile garnered significant media attention.²⁸ In response to BP’s complaints about the mock account, Twitter coerced the operator of the profile to post a disclaimer.²⁹ However, a response like Twitter’s may only go so far; as the population of social media sites has grown exponentially, efforts to control this problem and enforce trademark policies have been increasingly futile.

On June 5, 2009, Tony La Russa, the manager of the St. Louis Cardinals, filed a complaint against Twitter, accusing Twitter of cybersquatting.³⁰ The dispute centered on a Twitter profile that used La Russa’s name, had a picture of La Russa, and had a headline that said “Hey there! Tony La Russa is now using

BUSINESSWEEK (June 10, 2009, 12:01 AM EST), http://www.businessweek.com/technology/content/jun2009/tc2009069_767898.htm.

²⁵ *Id.*

²⁶ *Id.* See also Big Tent Democrat, *Obama, URLs, Domain Names, Cybersquatting and The First Amendment*, TALKLEFT.COM (May 2, 2007, 3:20 PM), <http://www.talkleft.com/story/2007/5/2/161947/9512> (noting that President Obama complained about an unofficial MySpace profile entitled “Friends of Obama,” which MySpace later transferred to his campaign).

²⁷ Brian Stelter, *BP Account on Twitter? Just a Joke; K thx bye*, N.Y. TIMES, June 10, 2010, <http://www.nytimes.com/2010/06/10/us/10twitter.html>. See also Maria Newman, *BlogTalk: Twitter and the G.O.P.*, THE CAUCUS (Oct. 22, 2009, 2:49 PM), <http://thecaucus.blogs.nytimes.com/2009/10/22/blogtalk-twitter-and-the-gop/> (discussing how Republican operatives created fake profiles with names like “MeetRepDonovan” and “MeetRepUrban”). Twitter shut down the account because the impersonation was intended to deceive voters and it confused voters, despite the disclaimer that the profile was sponsored by the state’s Republican Party. *Id.*

²⁸ Stelter, *supra* note 27.

²⁹ *Id.* Twitter’s policy allows users to pose as celebrities as long as they disclaim that the page is merely an impersonation and not intended to deceive anyone. See *id.*

³⁰ See Complaint at 2, *La Russa v. Twitter, Inc.*, No. CGC-09-488101, 2009 WL 1569936 (Cal. Super. Ct. May 6, 2009) [hereinafter Complaint, *La Russa*].

Twitter.”³¹ The profile encouraged users to “[j]oin today to start receiving Tony La Russa’s updates.”³² Unfortunately for the users who followed these tweets, the status updates were vulgar and derogatory.³³ La Russa argued that the author of the profile intended, in bad faith, to divert Internet traffic away from La Russa’s website and make a profit from the injury to La Russa’s mark.³⁴ La Russa’s case is the first of its kind, as no one has previously sued a social network site for cybersquatting.³⁵

La Russa v. Twitter, Inc. brings to the fore the issue of users reserving usernames and abusively using “hashtags”³⁶ that infringe upon famous brands. This Note argues that the username features on social networking sites have opened the door for a new form of cybersquatting and trademark infringement, one which extends beyond the infringement of personal names.³⁷ The vanity URLs and hashtags afford impostors with the opportunity to reserve famous brands as usernames and allow the impostor to use brands in hashtags to deceptively lure unsuspecting Internet users to an

³¹ Mark Milian, *Cardinals Manager Tony La Russa Sues Twitter for Imposter Account*, L.A. TIMES BLOG (June 4, 2009, 12:27 PM), <http://latimesblogs.latimes.com/technology/2009/06/tony-la-russa-twitter.html>.

³² Complaint, *La Russa*, *supra* note 30, at 3.

³³ *Id.*

³⁴ *Id.* at 4.

³⁵ See Macmillan, *supra* note 24. However, *La Russa v. Twitter* is not the first social media cybersquatting case; rather, the first case was *Thompson v. Clean Flicks Media*, in which a company sued an individual for reserving a MySpace username in bad faith. See Steven Seidenberg, *Name’s Sake: Social Media Pose Trademark Threats for Companies*, INSIDE COUNSEL (Sept. 1, 2009), <http://www.insidecounsel.com/Issues/2009/September-2009/Pages/Names-Sake.aspx>.

³⁶ A hashtag is a form of metatag, typically preceded by the “#” symbol, which allows users to categorize their tweets. *What are Hashtags?*, TWITTER HELP CENTER, <http://support.twitter.com/entries/49309-what-are-hashtags-symbols> (last visited Oct. 14, 2010). By categorizing their tweets, the hashtags allow tweets to show up in search engines. See *id.*

³⁷ Unlike other recent scholarly articles, the focus of this Note will be solely on username infringement of famous trademarks and brand names. See, e.g., Zorik Pesochinsky, *Almost Famous: Preventing Username Squatting on Social Networking Websites*, 28 CARDOZO ARTS & ENT. L.J., 223, 224–25 (2010) (discussing the implications of username infringement on personal names).

infringing profile. Such abusive registrations allow the impostor to make a profit off of the injury of a trademark and damage the reputation of a famous brand name.

However, the enforcement of trademark rights on social media websites could have a chilling effect on free speech rights and expose social media websites to frivolous lawsuits. Thus, enforcement must be limited. This Note maintains that both Twitter and Facebook need to expand their policies to include username infringement and hashtag infringement, and that Congress needs to amend the scope of the Anticybersquatting Consumer Protection Act (“ACPA”) to address many of the complex issues associated with trademark infringement on social media websites.

Part I of this Note will discuss the concept of cybersquatting and examine the ACPA.³⁸ Part II of this Note will explore the username features on Facebook and Twitter, illustrate the potential hazards that these features pose to the proprietary interests of trademark owners, and discuss whether the ACPA is applicable in the social networking arena. Part III will analyze the consequences of enforcing trademark rights on social media websites, specifically addressing free speech interests and contributory infringement. Finally, Part IV will propose legislative solutions to the problems associated with cybersquatting on social media websites.

I. THE CONCEPT OF CYBERSQUATTING AND ITS STATUTORY REMEDY

The pervasiveness of the Internet in everyday transactions has

³⁸ This Note will discuss the implications of the ACPA in the social networking arena, rather than focusing on the Uniform Domain Resolution Policy adopted by the Internet Corporation for Assigned Names and Numbers. *See* INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS, UNIFORM DOMAIN RESOLUTION POLICY (1999), *available at* <http://www.icann.org/en/udrp/udrp-policy-24oct99.htm>. Since the Uniform Domain Resolution Policy only focuses on second-level domain name infringement, and is not nearly as potent of a remedy as the ACPA (because its effects can merely be avoided by suing in federal court), it is not as relevant in this venue. *See* Seidenberg, *supra* note 35.

inevitably led to infringement of intellectual property.³⁹ The amount of Internet transactions has increased dramatically over the past decade, and companies have taken advantage of this venue by advertising and selling their products on the Internet.⁴⁰ With so many people browsing the Internet every day, it has become profitable for impostors to divert Internet users from their intended destinations thus diverting some of the business those users generate. These impostors rushed to register domain names that were remarkably similar to trademarks of corporations and, in doing so, left trademark owners powerless to protect their marks and register related domain names.⁴¹ In response to this practice, Congress took steps to give trademark owners protection rights on the Internet by enacting the ACPA in 1999.⁴² The statute gives trademark owners the power to seize domain names that are confusingly similar to their marks.⁴³

A. *The Concept of Cybersquatting*

There are many economic incentives for actors to engage in cybersquatting, but this practice often comes at the expense of trademark owners. The cybersquatter is typically able to divert the Internet user to the websites of a company's competitors.⁴⁴ These competitors pay the cybersquatter for each hit that they get on their websites.⁴⁵ In addition, because the trademark owner is unable to take advantage of his brand name, he is essentially forced to pay for the right to use his own brand name on the Internet⁴⁶ because the cybersquatter typically charges a fee to the trademark owner to

³⁹ See H.R. REP. NO. 106-412, at 6 (1999).

⁴⁰ *Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc.*, 202 F.3d 489, 493 (2d Cir. 2000)

⁴¹ See H.R. REP. NO. 106-412, at 6-7.

⁴² See MCCARTHY, *supra* note 12, §25:78.

⁴³ See *id.*

⁴⁴ *Id.* §25:77.

⁴⁵ See *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 765 (N.D. Ill. 2008).

⁴⁶ See *Sporty's Farm L.L.C.*, 202 F.3d at 493 (noting that mark owners are often "willing to pay 'ransom' in order to get 'their names' back") (citing H.R. REP. NO. 106-412, at 5-7; S. REP. NO. 106-140, at 4-7 (1999)).

transfer the domain name.⁴⁷

The process by which a cybersquatter harms the proprietary interests of trademark owners is important to understand.⁴⁸ The registration of a domain name similar to a brand name prevents the trademark owner from using his brand name in e-commerce because registration is done on a first come, first served basis.⁴⁹ By registering a domain name that is substantially similar to the owner's trademark, the cybersquatter precludes that owner from being able to use his brand name, which he likely spent a considerable amount of time building.⁵⁰ Thus, the trademark owner is unable to fully take advantage of his own brand name, which may result in a loss of potential profits.⁵¹ In addition, the registration of a website and reservation of relevant search terms prevent a trademark owner from having full control over his brand name and its reputation.⁵² By diverting the Internet user away from his intended destination, the Internet user can become confused and unsure of whether the website is legitimate.⁵³ Finally, the use of a mark in a domain name could essentially make a term generic, which would leave the term without any protection.⁵⁴

B. The Statutory Remedy to Cybersquatting

With the proliferation of Internet transactions in the 1990s and into the twenty-first century, cybersquatting became a widespread practice and trademark owners were left without a remedy to such

⁴⁷ *See id.* (“Cybersquatting involves the registration [of] domain names . . . by non-trademark holders who then try to sell the names back to the trademark owners.”).

⁴⁸ *See id.*

⁴⁹ *See id.*

⁵⁰ *See* H.R. REP. NO. 106-412, at 7.

⁵¹ *See id.* at 6.

⁵² *See id.*

⁵³ *Id.*

⁵⁴ *See* Jonathan J. Darrow & Gerald R. Ferrera, *The Search Engine Advertising Market: Lucrative Space or Trademark Liability?*, 17 TEX. INTELL. PROP. L.J. 223, 244–45 (2009) (“It is this same ability to convey meaning that underlies the great irony of trademark law—that too much success can bring ruin through genericide.”).

trademark infringement.⁵⁵ In response to this problem, Congress passed the Anticybersquatting Consumer Protection Act in 1999.⁵⁶ The ACPA served as an extension of the Lanham Act to protect trademark owners from infringement on the Internet by providing a trademark infringement cause of action for cases of cybersquatting. The statute applies only to top level domain names.⁵⁷ This new cause of action gives trademark owners an alternative to paying fees to cybersquatters to transfer domain names to the rightful owner and gives trademark owners the ability to enforce their rights on the Internet.⁵⁸

Under an ordinary trademark infringement claim, a trademark must be sufficiently distinctive or have acquired distinctiveness.⁵⁹ The ACPA incorporated the distinctiveness requirement of trademark law,⁶⁰ but added some additional requirements. In order to succeed on a cybersquatting claim, the plaintiff must

⁵⁵ MCCARTHY, *supra* note 12, § 25:77.

⁵⁶ *Id.* § 25:78.

⁵⁷ *See* *Hamptons Locations, Inc. v. Rubens*, 640 F. Supp. 2d 208, 213 (E.D.N.Y. 2009) (quoting *Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc.*, 202 F.3d 489, 493 (2d Cir. 2000)) (“[ACPA] ‘was passed to protect consumers and American businesses, to promote the growth of online commerce, and to provide clarity in the law for trademark owners by prohibiting the bad-faith and abusive registration of distinctive marks as Internet domain names with the intent to profit from the goodwill associated with such marks’”). ACPA defines a “domain name” as “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.” Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1127 (West 2006). As discussed later in this section, this could prove to be problematic for features such as hashtags. *See infra* Part IV.A.

⁵⁸ MCCARTHY, *supra* note 12, § 25:78.

⁵⁹ A trademark that is arbitrary, fanciful, or suggestive is inherently distinctive. *See generally* *Abercrombie & Fitch Co. v. Hunting World, Inc.*, 537 F.2d 4 (2d Cir. 1974). A descriptive term could be afforded the same protection as inherently distinctive marks if it obtains secondary meaning, in which the word is known by the public as specifically designating a particular product. *See Zatarain's, Inc. v. Oak Grove Smoke House*, 698 F.2d 786 (5th Cir. 1983) (noting that the term “FISH FRI” did obtain secondary meaning).

⁶⁰ *See, e.g., Venetian Casino Resort, LLC v. Venetiangold.com*, 380 F. Supp. 2d 737, 741–42 (E.D. Va. 2005) (discussing the ACPA’s requirement for distinctiveness of a mark).

demonstrate that the defendant registered or trafficked in a domain name that is (1) confusingly similar to plaintiff's mark and (2) that the defendant "had a bad faith intent to profit from the mark."⁶¹ The plaintiff's mark must be distinctive at the time of the registration of the domain name.⁶² Upon satisfying both criteria, the plaintiff is entitled to an *in rem* action consisting of the cancellation or transfer of the domain name to the rightful owner.⁶³

1. The Likelihood of Confusion

In order to state a successful cybersquatting claim, a plaintiff must demonstrate that the infringing domain name is confusingly similar to or dilutive of the plaintiff's mark.⁶⁴ In cybersquatting cases, confusingly similar means that the plaintiff's mark and the defendant's domain name are so similar "in sight, sound or meaning that they could be confused."⁶⁵ Courts analyze the likelihood of confusion in Internet cases using a two-step analysis; they consider (1) whether the marks are substantially similar and (2) the proximity of the goods and services.⁶⁶ The test, however, could end with the first step if the marks are identical or nearly identical.⁶⁷

⁶¹ Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1125(d)(1)(A) (West 2006).

⁶² *Id.* §1125(d)(2)(A).

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ MCCARTHY, *supra* note 12, § 25:78. Courts do not solely consider the similarity between domain names; rather courts also consider the similarity between the domain name and the plaintiff's trademark. *Id.*

⁶⁶ *See* *GoTo.com, Inc. v. Walt Disney Co.*, 202 F.3d 1199, 1205 (9th Cir. 2000). In *GoTo.com*, the court stated that in the Internet context, a likelihood of confusion analysis should entail an examination of (1) the similarity of the marks, (2) the proximity of the goods and services, and (3) the simultaneous use of the Web as a marketing channel. *Id.* This test is simpler than the seven factor tests employed in "standard" likelihood of confusion cases. *See, e.g.*, *Polaroid Corp. v. Polarad Elect. Corp.*, 287 F.2d 492, 497 (2d Cir. 1961). In *GoTo.com*, the court's third factor is rather redundant because, as the court admits, the two marks will likely be seen on the same screen. *See GoTo.com*, 202 F.3d at 1207. Therefore, this Note will not address the third factor.

⁶⁷ *See, e.g.*, *Texas Int'l. Prop. Assoc. v. Hoerbiger Holding AG*, 624 F.

Courts generally treat domain names that are substantially similar to a trademark as confusingly similar and thereby create a presumption of confusion.⁶⁸ A similarity in the appearance or sound of a mark could confuse consumers and this is relevant to the likelihood of confusion analysis.⁶⁹ For example, in *Texas International Property Associates v. Hoerbiger Holding AG*, the court held that the Texas International Property Association's "horbiger.com" was confusingly similar to Hoerbiger's mark because the domain name had nearly identical spelling to the Hoerbiger mark.⁷⁰ Likewise, in *People for Ethical Treatment of Animals v. Doughney*, the court maintained that defendant's domain name, "PETA.org," was a direct copy of plaintiff's mark and thus created a presumption of confusion on the part of Internet user.⁷¹ In both cases, the courts held that a substantial similarity between a domain name and a trademark creates the presumption of confusion and would eliminate the need to analyze the proximity of the goods and services.⁷²

Courts sometimes focus on the proximity between the goods and services that the domain name offers and those the trademarked company offers in order to ascertain whether Internet users are likely to be confused.⁷³ However, the proximity of the

Supp. 2d 582, 588 (N.D. Tex. 2009).

⁶⁸ *See id.*

⁶⁹ MCCARTHY, *supra* note 12, § 25:78.

⁷⁰ *See Texas Int'l*, 624 F. Supp. 2d at 591.

⁷¹ *People for Ethical Treatment of Animals v. Doughney*, 113 F. Supp. 2d 915, 919–20 (E.D. Va. 2000). Interestingly, the acronym used in the website was different from the plaintiff's mark (it stood for People Eating Tasty Animals), but the court held that this difference was immaterial. *Id.* at 918.

⁷² *See Texas Int'l*, 624 F. Supp. 2d at 588; *Doughney*, 113 F. Supp. 2d at 920.

⁷³ *Compare Hormel Foods Corp. v. Jim Henson Prods., Inc.*, 73 F.3d 497, 504 (2d Cir. 1996) (finding that the luncheon meat SPAM and the Muppets character Spa'am were dissimilar), *with GoTo.com, Inc. v. Walt Disney Co.*, 202 F.3d 1199, 1206–07 (9th Cir. 2000) (finding that "GoTo" and "Go Network" were similar where both entities operated web search engines). *See Jada Toys, Inc. v. Mattell, Inc.*, 518 F.3d 628, 632 (9th Cir. 2008) ("In the context of two subjectively dissimilar marks, evidence of actual confusion and evidence defining the context in which the goods are sold are particularly relevant.").

goods and services of a website arguably has nothing to do with the brand name in question.⁷⁴ For example, in *Cintas Corp. v. Unite Here*, the plaintiff was unable to prove that the disputed website, “cintasexposed.com” was confusingly similar to the CINTAS mark since there was “no proximity between the parties’ goods and services.”⁷⁵ The defendant’s website did not function as a source identifier; instead, the website served to “criticize Cintas’ corporate practices.”⁷⁶ Therefore, this second factor can either demonstrate consumer confusion, or it can establish that the website does not confuse consumers.

2. The Bad Faith Intent Requirement

In addition to the ACPA’s requirement for a likelihood of confusion, the plaintiff must also establish that the defendant intended, in bad faith, to profit from the plaintiff’s trademark by registering the domain name.⁷⁷ Congress designed the ACPA to “combat deliberate, bad faith, and abusive” registration of a domain name.⁷⁸ The ACPA includes a list of nine non-exclusive factors that allow the court to infer bad faith intent on the part of the impostor.⁷⁹ Under the safe harbor provision, if the court finds

⁷⁴ MCCARTHY, *supra* note 12, at § 25:78. McCarthy argues that this second factor is irrelevant for cybersquatting because many of these websites will not even be set up. *Id.* See also H.R. REP. NO. 106-412, at 6 (1999) (“These cyberpirates have no intention of using the domain name in commerce and instead often attempt to exact money from a company in exchange for domain names that relate to that company’s trademarks.”).

⁷⁵ *Cintas Corp. v. Unite Here*, 601 F. Supp. 2d 571, 579 (S.D.N.Y. 2009).

⁷⁶ *See id.*

⁷⁷ Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)(1)(A)(i) (West 2006).

⁷⁸ *Flentye v. Kathrein*, 485 F. Supp. 2d 903, 913–14 (N.D. Ill. 2007) (citing *Virtual Works, Inc. v. Volkswagen of America, Inc.*, 238 F.3d 624, 627 (4th Cir. 2001)) (internal quotation marks omitted).

⁷⁹ *See* 15 U.S.C.A. § 1125(d)(1)(A)(i). These bad faith factors include:

(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

that the defendant had reasonable grounds to believe that the domain name was available for fair use, then the defendant does not have the bad faith intent required by the ACPA.⁸⁰

Although courts will typically examine all of the ACPA elements for bad faith intent and determine if the elements favor either party, each element is not exclusive.⁸¹ When most of the elements cut in favor of the trademark owner, the court will infer bad faith intent.⁸² For example, in *Citigroup v. Chen Bao Shui*, the court held that defendant Chen Bao Shui's registration of the

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

Id.

⁸⁰ *Id.* § 1125(d)(1)(B)(ii).

⁸¹ *Id.* See, e.g., *Green v. Fornario*, 486 F.3d 100, 106 (3d Cir. 2007) (holding that since a majority of the elements favored Fornario, he had a "colorable defense" to the cybersquatting claim); *Audi AG v. D'Amato*, 469 F.3d 534, 549 (6th Cir. 2006) (maintaining that the majority of the elements cut against the defendant, thereby satisfying the bad faith intent requirement).

⁸² *Audi AG*, 469 F.3d at 549.

website “citybank.org” did not create intellectual property rights in the domain name.⁸³ Prior to the registration of the website, Chen Bao Shui did not use the domain name to offer any goods or services.⁸⁴ In addition, the court maintained that Chen Bao Shui intended to “confuse, mislead, and divert Internet traffic to garner click-through revenue” through false Citibank advertisements.⁸⁵ Finally, the court noted that Chen Bao Shui registered multiple domain names identical to Citibank’s marks.⁸⁶ When considering the ACPA’s bad faith factors, the court easily held that Chen Bao Shui acted in bad faith.⁸⁷

C. Trademark Infringement with Metatags

Trademark infringement on the Internet is not limited to cybersquatting and such infringement includes the abusive use of metatags.⁸⁸ However, the ACPA does not apply to metatags.⁸⁹ Indeed, the language of the ACPA provides an action only against an individual who “registers, traffics in, or uses a domain name.”⁹⁰ The ACPA defines a “domain name” as “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.”⁹¹ A metatag does not meet this definition because it is not assigned by a domain name registrar, but instead is entirely

⁸³ Citigroup, Inc. v. Chen Bao Shui, 611 F. Supp. 2d 507, 511 (E.D. Va. 2009).

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Id.* at 510–12 (noting that defendant registered multiple domain names similar to Citigroup’s registered marks: “Citibank,” “Citifield,” and “Citifinancial”).

⁸⁷ *Id.* at 512.

⁸⁸ See MCCARTHY, *supra* note 12, § 25:69.

⁸⁹ See Bihari v. Gross, 119 F. Supp. 2d 309, 316 (S.D.N.Y. 2000).

⁹⁰ Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1125(d)(A)(1)(ii) (West 2006) (emphasis added).

⁹¹ Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1127 (West 2006).

controlled by the web page creator.⁹²

Even though metatags fall outside of the scope of the ACPA, infringing use of such devices is still actionable under the Lanham Act.⁹³ The rationale for such protection is that the abusive use of metatags creates an initial interest problem: the consumer, who is deceptively lured to a competitor's website might choose to conduct business there rather than search for his intended destination.⁹⁴ Unlike with the ACPA, courts engage in the traditional lengthy likelihood of confusion analysis for metatag infringement, which typically consists of eight factors.⁹⁵ Passing this lengthy test is not easy,⁹⁶ but trademark owners nevertheless have recourse for metatag infringement.⁹⁷

⁹² See MCCARTHY, *supra* note 12, § 25:69.

⁹³ See *Wells Fargo & Co. v. WhenU.com, Inc.*, 293 F. Supp. 2d 734, 762 (E.D. Mich. 2003). However, some courts, such as the Second Circuit, do not entirely recognize metatag infringement as a trademark cause of action. See *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 414 F.3d 400, 409 (holding that "internal utilization of a trademark in a way that does not communicate it to the public" does not constitute "use" and thus does not violate the Lanham Act).

⁹⁴ See *Promatek Indus. Ltd. v. Equitrac Corp.*, 300 F.3d 808, 812 (7th Cir. 2002) ("Consumers who are directed to Equitrac's webpage [as a result of the infringing metatag] are likely to learn more about Equitrac and its products before beginning a new search for Promatek and Copitrak."); *Brookfield Commc'ns Inc. v. W. Coast Entm't Corp.*, 174 F.3d, 1036, 1064 (9th Cir. 2000) ("Using another's trademark in one's metatags is much like posting a sign with another's trademark in front of one's store.").

⁹⁵ See *N.Y. State Soc'y of Certified Pub. Accountants v. Eric Louis*, 79 F. Supp. 2d 331, 340 (S.D.N.Y. 1999) (citing *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492 (2d Cir. 1961)). The *Polaroid* factors for likelihood of confusion include:

- (1) the strength of the plaintiff's mark;
- (2) the degree of similarity between the two marks;
- (3) the competitive proximity of the products or services;
- (4) the likelihood that the plaintiff will "bridge the gap" between the two markets;
- (5) the existence of actual confusion;
- (6) the defendant's good faith in adopting its mark;
- (7) the quality of the defendant's product;
- and (8) the sophistication of the purchasers.

Id.

⁹⁶ See, e.g., *Bihari v. Gross*, 199 F. Supp. 2d, 309, 318–19 (S.D.N.Y. 2000) (finding that the abusive use of metatags did not create a likelihood of confusion).

⁹⁷ See *Promatek Indus. Ltd.*, 300 F.3d at 812 (holding a likelihood of confusion was probable after applying a seven factor likelihood of confusion

II. CYBERSQUATTING AND TRADEMARK INFRINGEMENT IN THE SOCIAL MEDIA ARENA

In light of the popularity of social media websites, corporations have created profiles on these websites to gain more customers.⁹⁸ Website administrators have extended the username feature to corporations who wish to use the feature to build a strong reputation for their marks.⁹⁹ Although Tony La Russa dropped his suit against Twitter, his case highlighted the hazards of the new username features on these websites.¹⁰⁰ The ACPA is applicable in the social networking venue, but prospective plaintiffs might have difficulty proving that defendant acted with the bad faith intent required by the ACPA.¹⁰¹

A. The Hazards of Name Squatting and Hashtag Infringement

1. Name Squatting: Why it Matters

The reservation of usernames and the abusive use of tags are particularly harmful to trademark owners. Facebook admits that username infringement can “be a big deal[,] especially if someone else is looking to build a reputation using a brand name that you’ve spent a long time building.”¹⁰² Cybersquatting via username infringement prevents the trademark owner from using that recognizable username, and thereby inhibits his ability to use his brand name on that particular social media website.¹⁰³ Reserving a username, much like reserving a domain name, allows the

test); *N.Y. State Soc’y of Certified Pub. Accountants*, 79 F. Supp. 2d at 340–42 (holding that the infringing use of metatags passed the *Polaroid* test).

⁹⁸ See William McGeeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1119 (2009) [hereinafter, McGeeveran, *Disclosure*].

⁹⁹ See *id.*

¹⁰⁰ See MacMillan, *supra* note 24.

¹⁰¹ See *infra* Part II.C.

¹⁰² Nick O’Neill, *How to Get Your Facebook Username Back From a Squatter*, ALLFACEBOOK (June 22, 2009, 10:04 AM), <http://www.allfacebook.com/2009/06/facebook-username-squatter/>.

¹⁰³ See *id.*

impostor to prevent the trademark owner from using his brand name in a useful market.¹⁰⁴

Moreover, the reservation of a username by an impostor can tarnish and dilute the reputation of the mark. When someone reserves a username in bad faith, the trademark owner loses control over the reputation of his brand name. For example, in *Clean Flicks, Inc. v. Daniel Dean Thompson*, the defendant's cybersquatting tainted the Clean Flicks mark.¹⁰⁵ Specifically, the defendant registered Clean Flicks Media as his username on Myspace and tried to pass himself off as one of the founders of the company.¹⁰⁶ The problem with this reservation was that the defendant was arrested for possession of child pornography, statutory rape, and other crimes which were completely at odds with Clean Flicks' reputation as a family entertainment business.¹⁰⁷ In the immediate aftermath of the arrest, news stories linked Clean Flicks Media to the defendant because of the Myspace page,¹⁰⁸ and Clean Flicks had to sue in order to defend its reputation.¹⁰⁹ Therefore, reserving usernames leaves trademark owners without control over the reputation of their marks, which could be detrimental to the mark's power.

¹⁰⁴ See *Help Center*, FACEBOOK, <http://www.facebook.com/help/?page=897> (last visited Sept. 25, 2010) (explaining that users must choose a "unique" username). See, e.g., *Morrison & Foerster, LLP v. Wick*, 94 F. Supp. 2d 1125, 1126–27 (D. Colo. 2000) (discussing how registering a domain name precludes trademark owners from using their brand names). See generally *McGeveran, Disclosure*, supra note 98 (discussing the value of social media as a medium for marketing).

¹⁰⁵ See Complaint at 6, *Clean Flicks, Inc. v. Daniel Dean Thompson*, No. 2:08-cv-0086-PMW (D. Utah Feb. 1, 2008) available at <http://www.schwimmerlegal.com/Complaint%20clean%20flicks.pdf> [hereinafter Complaint, *Clean Flicks*]. See also Nate Anderson, *Sex, Drugs, and Dirty Movies: CleanFlicks Sues Doppelganger*, ARS TECHNICA (Feb. 5, 2008), <http://arstechnica.com/tech-policy/news/2008/02/sex-drugs-and-dirty-movies-cleanflicks-sues-cyberpirate.ars>.

¹⁰⁶ *Id.*

¹⁰⁷ Complaint, *Clean Flicks*, supra note 105, at 4; Anderson, supra note 105.

¹⁰⁸ Complaint, *Clean Flicks*, supra note 105, at 4.

¹⁰⁹ See Anderson, supra note 105.

2. The Dangers of Hashtag Infringement

Much like name squatting, hashtag infringement is a significant problem on Twitter. Hashtags, much like metatags, allow individuals to place words in their profiles and on tweets, which in turn show up on search engines.¹¹⁰ By allowing individuals free control over the content of their tags in tweets, individuals have abused this feature and in turn, inflicted harm on the power and distinctiveness of a brand name.

Taco John's is one of the more recent victims of infringing use of hashtags. In August 2010, Taco John's sent a cease and desist letter to Iguana Grill for their usage of the hashtag "#tacotuesday," which they maintained was an infringing use of their registered trademark "Taco Tuesday."¹¹¹ However, sending this letter backfired on Taco John's as the story garnered media attention; individuals began to use the hashtag freely in their tweets and due to the media attention, Iguana sold a record number of tacos in one day.¹¹²

The Taco John's example demonstrates the dangers of an infringing use of a hashtag. Although hashtag use does not preclude the trademark owner from using the mark,¹¹³ the free use of a brand name in a hashtag can dilute the trademark or possibly even lead to genericide.¹¹⁴ The more freely a brand, such as "Taco Tuesday," is used, the less likely consumers will recognize the term as a source identifier.¹¹⁵ When a term loses its function as a source identifier, the trademark becomes generic and loses its distinctiveness.¹¹⁶ Without distinctiveness, a trademark is not entitled to protection.¹¹⁷

¹¹⁰ *What are Hashtags?*, TWITTER HELP CENTER, <http://support.twitter.com/entries/49309-what-are-hashtags-symbols> (last visited Oct. 14, 2010).

¹¹¹ See Emily E. Campbell, *Taco John's Claims Rights in Taco Tuesday*, PHOSITA: AN INTELLECTUAL PROPERTY BLOG (Aug. 4, 2010), <http://dunlapcoding.com/phosita/2010/08/taco-johns-claims-rights-in-taco-tuesday.html>.

¹¹² See *id.*

¹¹³ MCCARTHY, *supra* note 12, §25:69.

¹¹⁴ See *id.*

¹¹⁵ See Darrow & Ferrera, *supra* note 54, at 244–45.

¹¹⁶ See *id.*

¹¹⁷ See *id.*

*B. Efforts to Curtail Username Infringement**1. Facebook's Policy*

In an effort to learn from and avoid the pitfalls of Twitter's and Myspace's lax guidelines with username features, Facebook implemented safeguards to protect trademark owners on its website.¹¹⁸ Facebook reserves the right to reclaim usernames on the website if they infringe on a trademark.¹¹⁹ Trademark owners are responsible for reporting any trademark infringement on a username infringement form Facebook provides.¹²⁰ On the form, trademark owners are expected to provide proof of registration and explain how the username infringes on their mark.¹²¹ If the trademark owner successfully establishes infringement, then Facebook will transfer the username to the trademark owner.¹²²

Facebook also encouraged trademark owners to reserve usernames before the launch of the feature on June 13, 2009.¹²³ To reserve a username before June 13, users had to have at least one thousand followers, which is a difficult task for a cybersquatter to achieve.¹²⁴ New users were otherwise not permitted to register until June 28, 2009 to prevent people from creating multiple

¹¹⁸ See Macmillan, *supra* note 24.

¹¹⁹ See Blaise DiPersia, *Coming Soon: Facebook Usernames*, THE FACEBOOK BLOG (June 9, 2009, 12:11PM), <http://blog.facebook.com/blog.php?post=90316352130>; see also *Help Center*, FACEBOOK, <http://www.facebook.com/help/?page=897> (last visited Sept. 25, 2010) (explaining that Facebook will reclaim any username that it determines to be squatting).

¹²⁰ See *Report an Infringing Username*, FACEBOOK, http://www.facebook.com/help/contact.php?show_form=username_infringement (last visited Sept. 25, 2010).

¹²¹ See *id.*

¹²² See *id.*

¹²³ Facebook Pages, *Facebook Usernames Coming Soon for Pages*, FACEBOOK (June 9, 2009, 4:32 PM), <http://blog.facebook.com/blog.php?post=90316352130>.

¹²⁴ See generally "New Facebook Policy Could Invite Cybersquatting," INDIANAPOLIS BUSINESS JOURNAL, Jun. 22, 2009 (discussing how many experts agree that the risk of classic cybersquatting is rather minimal in this venue).

accounts to reserve usernames in bulk.¹²⁵ In addition, when the username feature launched in 2009, Facebook allowed certain users, namely corporations, to flag certain names that might conflict with the owner's trademark.¹²⁶

Facebook has a verification feature to prevent any future harm to brand names.¹²⁷ In an attempt to avoid "name squatting," Facebook announced that usernames may now require "mobile phone authentication."¹²⁸ Thus, in order to obtain a username, the individual might need to verify the account by phone. It remains to be seen whether Facebook will stringently enforce such verification. It is also not clear what other loopholes may appear in this approach; for example, whether the cybersquatter could still pose as the trademark owner if Facebook were to contact him.

2. Twitter's Policy

Twitter has also created a verification feature to prevent confusion.¹²⁹ Twitter maintains that it created the feature to "establish authenticity for accounts who deal with identity confusion regularly on Twitter."¹³⁰ Unlike Facebook, Twitter uses "verification badges" which signal to users that the profile is not fake.¹³¹ Interestingly, Twitter's mechanism does not yet apply to all businesses, as the website is currently testing a verification feature for businesses.¹³² Currently, the feature is available only to "public officials, public agencies, famous artists, athletes, and other well known individuals at risk of impersonation."¹³³ Some

¹²⁵ *See id.*

¹²⁶ Facebook Pages, *supra* note 123.

¹²⁷ *See Macmillan, supra* note 24.

¹²⁸ *Help Center*, FACEBOOK, *supra* note 104.

¹²⁹ *See About Verified Accounts*, TWITTER, <http://support.twitter.com/groups/31-twitter-basics/topics/111features/articles/119135-about-verified-accounts> (last visited Sept. 25, 2010).

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *Business Verification*, TWITTER, <http://twitter.zendesk.com/76487-can-i-verify-my-business-account> (last visited Sept. 15, 2010).

¹³³ Emma Barnett, *Twitter Launches Verification Service to Protect Celebrities*, TELEGRAPH (June 8, 2009, 11:04 AM BST), <http://www.telegraph>.

corporations have access to the verification feature during the testing period, but at this point, many are not able to benefit from this feature.¹³⁴

A search of Twitter reveals that corporations are susceptible to username infringement, especially those owning famous brand names.¹³⁵ When Twitter first created its username feature, cybersquatters scrambled to reserve usernames that were substantially similar or identical to famous brand names.¹³⁶ In 2009, impostors reserved usernames such as Volkswagen,¹³⁷ which Twitter has since transferred to the rightful owners.¹³⁸ One of the more notable examples was “@Hyundai,” a profile that contained pictures of scantily clad woman and telling users to “have a lustful day.”¹³⁹ After Hyundai threatened to sue Twitter over the profile,¹⁴⁰ the site’s administrators transferred the username to the

co.uk/technology/twitter/5475445/Twitter-launches-verification-service-to-protect-celebrities.html (internal quotation marks omitted).

¹³⁴ See *Business Verification*, TWITTER, *supra* note 132. For example, Target has a verified business account. See *Target*, TWITTER, <http://twitter.com/target> (last visited Sept. 15, 2010).

¹³⁵ Willis Wee, *10 Brands Claimed by Twitter Cybersquatters*, PENN-OLSON (Sept. 21, 2009), <http://www.penn-olson.com/2009/09/21/10-brands-claimed-by-twitter-cybersquatters/> (discussing various brand names that succumbed to name squatting). One of these fake profiles had over 1,000 followers during 2009, but many of these usernames have either been suspended or transferred to the rightful owners. *Id.* The lack of activity (many have no tweets) on these pages serves as evidence that these profiles are held by impostors.

¹³⁶ See *id.*

¹³⁷ *Id.*

¹³⁸ See *Volkswagen*, TWITTER, <http://twitter.com/volkswagen> (last visited Sept. 15, 2010). Previously, the owner of the profile solicited bids for individuals to purchase the username “@volkswagen.” See Wee, *supra* note 135. However, the profile now contains the company’s logos, directs customers to the official Volkswagen website, has over 600 tweets, and has close to 9,000 followers. See *Volkswagen*, TWITTER, <http://twitter.com/volkswagen> (last visited Sept. 15, 2010). Thus, the profile has clearly been transferred to Volkswagen.

¹³⁹ Stephen Calogera, *Hyundai Falls Victim to Cybersquatters on Twitter*, EGM CARTECH (Nov. 10, 2009), <http://www.egmcartech.com/2009/11/10/hyundai-falls-victim-to-cyber-squatters-on-twitter/>.

¹⁴⁰ *Id.*

company.¹⁴¹ However, the problem still exists, as impostors currently reserved famous brand names including Apple,¹⁴² Macbook,¹⁴³ Carvel,¹⁴⁴ Nike,¹⁴⁵ Adidas,¹⁴⁶ Ikea,¹⁴⁷ Neiman Marcus,¹⁴⁸ and DSquared.¹⁴⁹ Thus, cybersquatters have abused and continue to abuse the username feature on Twitter.

In light of the wave of these fake profiles, Twitter amended its policy. Much like the username infringement form on Facebook, companies can complain to the site's administrators about a case of username infringement.¹⁵⁰ Twitter requires that in order for there to be name squatting, the account must be active and that there have been "attempts to sell, buy, or solicit other forms of payment in exchange for usernames."¹⁵¹ Conversely, accounts without status updates that contain no profile image typically indicates "that there's no name-squatting or impersonation."¹⁵²

For non-cybersquatting cases, Twitter has a catch-all trademark policy.¹⁵³ Trademark owners can report any infringing use of their

¹⁴¹ See *Hyundai*, TWITTER, <http://twitter.com/hyundai> (last visited Sept. 15, 2010). Hyundai now owns this username and profile. See Calogera, *supra* note 139.

¹⁴² See *Apple*, TWITTER, <http://twitter.com/Apple> (last visited Sept. 15, 2010).

¹⁴³ See *Macbook*, TWITTER, <http://twitter.com/macbook> (last visited Sept. 15, 2010).

¹⁴⁴ See *Carvel*, TWITTER, <http://twitter.com/carvel> (last visited Sept. 15, 2010).

¹⁴⁵ See *Nike*, TWITTER, <http://twitter.com/nike> (last visited Sept. 15, 2010). See also *Nik!*, MYSPACE, <http://myspace.com/nike> (last visited Sept. 15, 2010).

¹⁴⁶ See *Adidas*, TWITTER, <http://twitter.com/adidas> (last visited Sept. 15, 2010).

¹⁴⁷ See *Ikea*, TWITTER, <http://twitter.com/ikea> (last visited Sept. 15, 2010).

¹⁴⁸ See *Neiman Marcus*, TWITTER, <http://twitter.com/neimanmarcus> (last visited Sept. 15, 2010).

¹⁴⁹ See *Dsquared*, TWITTER, <http://twitter.com/dsquared> (last visited Sept. 15, 2010).

¹⁵⁰ See *Name Squatting Policy*, TWITTER HELP CENTER, <http://support.twitter.com/articles/18370-name-squatting-policy> (last visited Sept. 15, 2010).

¹⁵¹ *Id.*

¹⁵² *Id.*

¹⁵³ See *Trademark Policy*, TWITTER HELP CENTER, <http://support.twitter.com/entries/18367> (last visited Oct. 15, 2010).

marks to Twitter's administrators.¹⁵⁴ Because Twitter does not want to inhibit free speech and expression on news feeds and hashtags, the administrators do "not actively monitor users' content and will not edit or remove user content."¹⁵⁵ Rather, the trademark owners are expected to police their marks and report any infringing use.¹⁵⁶ When reporting infringing use of a mark on devices such as hashtags, the trademark owner must provide proof of registration.¹⁵⁷ Unregistered marks are not protected under this mechanism.¹⁵⁸

Currently, it appears that Twitter vigorously enforces this policy. For example, in December 2009, after receiving complaints about an infringing username on the Heinz trademark, Twitter changed the username without consulting the profile owner.¹⁵⁹ Likewise, Twitter transferred the Hyundai username to the rightful owners after the company complained.¹⁶⁰ Even with such enforcement, however, the policy is reactive rather than proactive. Companies must wait until the infringement has occurred before they may file a complaint.¹⁶¹ In that period of time, the damage may already have occurred, as it had with the BP and Clean Flicks profiles.¹⁶² Therefore, although companies have options to protect their brand names, Twitter's current policy does little to protect them from trademark infringement and potential harm to their brand names.

¹⁵⁴ *Id.*

¹⁵⁵ *See id.*

¹⁵⁶ *See id.*

¹⁵⁷ *Id.*

¹⁵⁸ *See id.*

¹⁵⁹ Jason Turbow, *The Great Ketchup Experiment: Cybersquatting and the Power of Social Media*, BAYNEWSEER (Feb. 17, 2010, 12:57 PM), http://www.mediabistro.com/baynewser/twitter/the_great_ketchup_experiment_cybersquatting_and_the_power_of_social_media_152333.asp (discussing how Twitter transferred the username "HJ Heinz" to "NotHJ_Heinz").

¹⁶⁰ *See Hyundai*, TWITTER HELP CENTER, *supra* note 141; *see also Calogera*, *supra* note 139.

¹⁶¹ *See Name Squatting Policy*, TWITTER, *supra* note 150.

¹⁶² *See supra* text accompanying notes 27–29, 105–109.

C. ACPA and Username Infringement

The ACPA, enacted over ten years ago, addressed the abusive registration of full quality domain names.¹⁶³ Legislators, however, did not foresee the launch and exponential growth of the Internet during the “Web 2.0” phenomenon; such lack of foresight is evident with the limitation of the ACPA to top level domain names.¹⁶⁴ In light of this new venue, the ACPA, while somewhat dated, nevertheless gives trademark owners a remedy to such abusive registrations.¹⁶⁵

1. The Likelihood of Confusion

With the growth of popularity in social networking websites, one must wonder whether, in this context, username infringement is likely to cause any confusion among consumers. As a marketing channel, the Internet “is particularly susceptible to a likelihood of confusion since . . . it allows for competing marks to be encountered at the same time, on the same screen.”¹⁶⁶ The search costs of stumbling on an impostor’s profile, however, are rather minimal; the Internet user merely has to click the back button to leave the page.¹⁶⁷

Under the ACPA, courts do not address “whether the accused domain name is confusingly similar to the plaintiff’s domain name, but whether it is confusingly similar to the plaintiff’s trademark or

¹⁶³ MCCARTHY, *supra* note 12, § 25:78.

¹⁶⁴ See O’Reilly, *supra* note 2 (describing the rise of personal homepages during the Web 2.0 phenomenon). Such websites would not include top level domain names. Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1127 (West 2006) (“The term ‘domain name’ means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.”).

¹⁶⁵ In light of Web 2.0 and increased user control, see O’Reilly, *supra* note 2 (discussing increased user control in the Web 2.0 phenomenon), this Note argues for an expansion of the definition of “domain name.” See *infra* Part IV.A.

¹⁶⁶ GoTo.com, Inc. v. Walt Disney Co., 202 F.3d 1199, 1207 (9th Cir. 2000).

¹⁶⁷ See *id.* at 1209.

service mark.”¹⁶⁸ Thus, a vanity URL that is confusingly similar to a plaintiff’s trademark would satisfy the first requirement of the ACPA.¹⁶⁹ Because vanity URLs function as domain names,¹⁷⁰ an infringement claim for name squatting would mirror the likelihood of confusion analysis with domain names.¹⁷¹

2. *Bad Faith Intent on Social Media Websites*

Congress created the ACPA to prevent abusive registrations of domain names.¹⁷² On the one hand, some evidence that judges use to ascertain whether a defendant abusively registered a domain name in bad faith will be applicable to this analysis in the username context.¹⁷³ On the other hand, the reservation of one’s nickname as a username presents judges with a unique problem in evaluating the bad faith element.¹⁷⁴

Nicknames could present courts with a problem in determining whether an individual reserved a username in bad faith. Myspace, Twitter, and Facebook allow their users to reserve usernames, which serve as URL shortcuts to a profile.¹⁷⁵ Such usernames can conflict with famous marks, particularly if the mark and nickname are similar. For example, an individual on Myspace reserved the username “Nike” because his nickname is “Nik. E.”¹⁷⁶ The

¹⁶⁸ MCCARTHY, *supra* note 12, § 25:78.

¹⁶⁹ *See id.* For a full discussion of the “presumption of confusion” standard, see *infra* Part I.B.1.

¹⁷⁰ *GoTo.com, Inc.*, 202 F.3d at 1207; *see also* Wakiyama and Kagan, *supra* note 18 (discussing how Facebook usernames function as URLs).

¹⁷¹ *See* Texas Int’l. Prop. Assoc. v. Hoerbiger Holding AG, 624 F. Supp. 2d 582, 588 (N.D. Tex. 2009); People for Ethical Treatment of Animals v. Doughney, 113 F. Supp. 2d 915, 919–20 (E.D. Va. 2000).

¹⁷² MCCARTHY, *supra* note 12, § 25:78.

¹⁷³ *Id.*

¹⁷⁴ *Id.*

¹⁷⁵ *See supra* text accompanying notes 18–20.

¹⁷⁶ Many users on Myspace have registered usernames that are substantially similar to famous brands. *See, e.g., Nik!*, MYSPACE, *supra* note 145. On this profile, the user seems to have reserved a nickname. *Id.* On others, the user seems to have reserved the famous brand name as an online nickname, but is not one that he is commonly referred to. *See, e.g., Doddio*, MYSPACE, <http://www.myspace.com/stopnshop> (last updated Feb. 11, 2010, 2:58 AM).

reservation of this username was performed in good faith, but it prevents Nike from using its trademark on Myspace.¹⁷⁷

The legal name safe harbor of the ACPA merely provides a court with “the appropriate discretion to determine whether or not the fact that a person bears a nickname similar to a mark at issue is an indication of an absence of bad-faith on the part of the registrant.”¹⁷⁸ The crafters of the ACPA of course did not intend for this provision to permit users to make up a nickname that is substantially similar to a well-known brand name.¹⁷⁹ However, individuals could attempt to reserve a domain name with a “word that they claim as a ‘nickname’ which is allegedly ‘commonly used’ to refer to them, but which is very similar to that of a well-known trademark.”¹⁸⁰

A legal name would fall under the safe harbor provision of the ACPA because the applicant could have registered the username in good faith.¹⁸¹ A person, however, could also assert that they use a commonly used word as a nickname, which also happens to be similar to a trademark.¹⁸² Such username reservations would present judges with a situation in which it would not be clear whether the username was reserved in bad faith.¹⁸³ Some users will obviously do this in bad faith and assert that their use of the nickname falls under the safe harbor provision.¹⁸⁴ Fortunately, one may not assert a good faith claim under the safe harbor provision after the dispute over the username arises.¹⁸⁵ The line between

¹⁷⁷ See *Nik!*, MySpace, *supra* note 145.

¹⁷⁸ MCCARTHY, *supra* note 12, § 25:78 (citing H.R. Rep. No. 106-412, at 10 (1999)).

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

¹⁸¹ See, e.g., *Int’l Bancorp v. Societe des Bains de Mer et du Cercle des Etrangers a Monaco*, 192 F.Supp. 2d 467,485 (E.D. Va. 2002) (“A putative cyberpirate can satisfy this factor only if its name or commonly-used nickname is the same as the domain name in dispute.”). A legal name is generally a person’s name. See *id.*

¹⁸² *Id.*

¹⁸³ MCCARTHY, *supra* note 12, § 25:78.

¹⁸⁴ See *id.* (“For example, consider the hypothetical Roberto Wayne who registers the domain name sonywalkman.net and who claims that this is justified because his friends call him “sony” and that he is a man who walks a lot.”).

¹⁸⁵ See *id.* A good faith claim “cannot be founded upon some purported

such claims, however, would be rather blurry. Courts will be forced to choose between a person's right to use his nickname in a social setting against the proprietary interests of the trademark owner.¹⁸⁶ Ascertaining whether someone used that nickname in good faith would entail an examination as to how extensively the impostor used the nickname in the past and whether he created the nickname to be identified with a particular source.¹⁸⁷ Such an examination, however, would be difficult and expensive.¹⁸⁸

III. THE CONSEQUENCES OF ENFORCING TRADEMARK RIGHTS ON SOCIAL NETWORKING WEBSITES

Although there are loopholes that allow users to reserve a username that infringes on a famous brand name, trademark owners still have options to protect their rights.¹⁸⁹ There are two problems with allowing individuals to sue for trademark infringement in social media websites. First, trademark owners might become too strategic in their enforcement of their trademark rights by suing the social media websites for infringement. Second, trademark owners will overly enforce their trademark rights to the point that it will stifle speech in a socially valuable setting. Given the redressability of trademark rights, the enforcement of these rights must be limited in order to avoid frivolous lawsuits and impermissible infringement on free speech.

A. Contributory Infringement by Social Networking Sites

In La Russa's complaint, he accused Twitter of cybersquatting via contributory infringement.¹⁹⁰ La Russa would likely have lost his case, as registration sites, such as Twitter, are generally not

good faith use of the domain name undertaken only after the dispute arose and motivated by a desire to fabricate a good faith defense." *Id.*

¹⁸⁶ See *id.* See *infra* Part III.B, for a fuller discussion of this tension.

¹⁸⁷ See *Int'l Bancorp*, 192 F. Supp 2d at 485.

¹⁸⁸ *Id.*

¹⁸⁹ See *id.*

¹⁹⁰ See Complaint, *La Russa*, *supra* note 30, at 2 (arguing that since Twitter maintained the domain name, it was contributorily liable for third party infringement).

liable for violations of the ACPA.¹⁹¹ Judges do not recognize contributory liability for registration sites because the operator of the registration site has no role in creating the website's content.¹⁹² The ACPA strictly limits liability for "the domain name registrant or that registrant's authorized licensee" when registering infringing domain names.¹⁹³ Registration sites, therefore, are not the appropriate defendants for such lawsuits.

In the social networking setting, La Russa's claim against Twitter should be precluded by Section 230 of the Communications Decency Act ("CDA"),¹⁹⁴ a statute that deals primarily with defamatory or otherwise illegal content.¹⁹⁵ The CDA states that no "provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."¹⁹⁶ A social networking site, which is a provider of interactive computer service, would thus be immune under this statute.¹⁹⁷ Some courts have refused to grant this immunity for Interactive Service Providers ("ISPs") where the administrator "edits in a manner that contributes to the alleged illegality."¹⁹⁸ However, when an interactive service provider uses neutral tools that incidentally assist the alleged illegality, the ISP will generally be immune from liability.¹⁹⁹ Invoking this analysis, a social

¹⁹¹ *American Girl, LLC v. Nameview, Inc.*, 381 F. Supp. 2d 876, 881 (E.D. Wis. 2005) ("[R]egistrars are not obliged to examine domain names to ensure that the registrant is not violating the rights of a third party.").

¹⁹² *Parker v. Google*, 422 F. Supp. 2d 492, 503 (E.D. Pa. 2006); *but see* *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 765 (N.D. Ill. 2008) (holding that Google could be held liable for third party infringement because they allegedly paid registrants for registering infringing domain names).

¹⁹³ Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)(1)(D) (West 2006).

¹⁹⁴ *See* MacMillan, *supra* note 24.

¹⁹⁵ *Id.*

¹⁹⁶ Communications Decency Act, 47 U.S.C.A. § 230(c) (West 1998).

¹⁹⁷ *See* MacMillan, *supra* note 24 (noting that Google, MySpace, AOL, and Craigslist are immune under CDA).

¹⁹⁸ *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1169 (9th Cir. 2008).

¹⁹⁹ *E.g.*, *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 670–71 (7th Cir. 2008).

networking website would generally be liable if the administrators edited the content of the username or profile in a way which created infringement.²⁰⁰ Neutral mechanisms, like the registration of a username, would not be sufficient under this analysis.²⁰¹

La Russa cleverly avoided this immunity provision by asserting a cybersquatting claim.²⁰² Under Section 230(e) of the CDA, the immunity provision is not intended to “limit or expand” intellectual property law.²⁰³ A trademark infringement claim such as La Russa’s would circumvent this immunity provision because the claim would be predicated on trademark infringement, and Section 230(e) provides that the immunity provision should not be construed to limit trademark law. On the one hand, by granting outright immunity to any ISP, trademark owners would have no relief against websites that are complicit with infringing activities.²⁰⁴ From a policy perspective, however, granting a trademark cause of action against a social networking website is troubling, for it seems to undermine the spirit of CDA.²⁰⁵ By asserting a cybersquatting or metatag infringement claim, a plaintiff would be able to preclude immunity and sue social networking sites for third party infringement.²⁰⁶

Despite these problems, judges do not tend to recognize such claims against neutral third party websites.²⁰⁷ The ACPA does not mention secondary liability and thus this theory is primarily derived from the common law.²⁰⁸ Similar to the analysis under the

²⁰⁰ *Fair Hous. Council*, 521 F.3d at 1169.

²⁰¹ *Id.*

²⁰² See Complaint, *La Russa*, *supra* note 30, at 4 (arguing that since Twitter maintained the domain name, it was contributorily liable for third party infringement).

²⁰³ Communications Decency Act, 47 U.S.C.A. § 230(e)(2) (West 1998).

²⁰⁴ See *MacMillan*, *supra* note 24.

²⁰⁵ 47 U.S.C.A. § 230(c).

²⁰⁶ *Id.*

²⁰⁷ See *Lockheed Martin v. Network Solutions, Inc.*, 194 F.3d 980, 983 (9th Cir. 1999).

²⁰⁸ See, e.g., *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.* 456 U.S. 844, 855 (1982) (establishing the rule for contributory infringement for products); *Lockheed Martin*, 194 F.3d at 983 (discussing the rule for contributory infringement for services).

CDA, domain registration sites²⁰⁹ generally cannot be held liable for contributory infringement because the registration of websites typically does not entail intentional inducement to create infringing products on a mark.²¹⁰ The court in *Lockheed Martin v. Network Solutions* held that third parties offering services must have direct control and monitoring over the instrumentality in order to be held liable.²¹¹ Likewise, in *Tiffany v. eBay*, a case involving counterfeit goods, the Second Circuit held that in order for there to be contributory infringement, “a service provider must have more than a general knowledge or a reason to know that its service is being used to sell counterfeit goods.”²¹² Rather, the court reasoned that the “contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary.”²¹³

Under the *Tiffany* standard, social networking sites would not be liable for cybersquatting if the administrators did not have specific and contemporary knowledge of the trademark infringement.²¹⁴ Without specific knowledge, there would not be direct control over the instrumentalities, the requirement articulated by the court in *Lockheed-Martin*.²¹⁵ Even with specific knowledge, if the website takes reasonable steps to curtail the infringement, as eBay did, then the website cannot be held contributorily liable for cybersquatting.²¹⁶ Without specific knowledge or inaction, there would be no intentional inducement and thus no contributory infringement.²¹⁷ Consequently, unless a social networking site monitors and controls the reservation of an infringing username, and makes no effort to ameliorate the

²⁰⁹ See, e.g., REGISTER.COM, <http://www.register.com/> (last visited Sept. 16, 2010). A domain registration site allows an individual to reserve a domain name or renew an expired domain name, and even offers services such as search engine optimization. See *id.*

²¹⁰ See *Lockheed Martin*, 194 F.3d at 983.

²¹¹ *Id.* at 985.

²¹² *Tiffany (N.J.), Inc. v. eBay, Inc.*, 600 F.3d 93, 107 (2d Cir. 2010).

²¹³ *Id.*

²¹⁴ See *id.*

²¹⁵ See *Lockheed Martin*, 194 F.3d at 985 (9th Cir. 1999)

²¹⁶ *Tiffany*, 600 F.3d at 107–10.

²¹⁷ *Id.* at 107.

problem, the site should not be held liable.²¹⁸

B. Effects on Free Speech Rights on the Internet

The enforcement of trademark rights regulates use of a mark to prevent dilution or genericide of the mark.²¹⁹ The First Amendment of the Constitution, on the other hand, affords individuals the right to free speech, which gives individuals the right to express themselves for political and social reasons, among others.²²⁰ In contrast, trademark law is about preventing the use of a word, slogan, or design by someone other than the mark owner.²²¹ In the context of social media websites, the regulation of both username vanity URLs and hashtags would prevent people from using a particular mark in a social setting, where the First Amendment generally protects expression.²²² The protection of a trademark and the right to free speech are therefore at odds with one another. The monopolization of a popular term, particularly one with cultural significance, could stifle artistic expression, criticism, and other social speech.²²³

The general rule for free speech in trademark law is that if the use of the mark in speech is noncommercial or nominative it will not pose a threat to the trademark owner's interests.²²⁴ The courts currently define "commercial speech" as speech that "does no more than propose a commercial transaction" in a manner "removed from any exposition of ideas."²²⁵ Noncommercial speech

²¹⁸ *See id.*

²¹⁹ William McGeeveran, *Four Free Speech Goals for Trademark Law*, 18 *FORDHAM INTELL. PROP. MEDIA & ENT. L.J.* 1205, 1225 (2008) [hereinafter McGeeveran, *Four Free Speech Goals*].

²²⁰ U.S. CONST. amend. I.

²²¹ *See* McGeeveran, *supra* note 219.

²²² *See supra* Part II.A.

²²³ *See* William McGeeveran, *Rethinking Trademark Fair Use*, 94 *IOWA L. REV.* 49, 65–66 (2008) [hereinafter McGeeveran, *Rethinking Trademark Fair Use*].

²²⁴ *See* *New Kids on the Block v. News Am. Publ'g, Inc.*, 971 F.2d 302, 308 (9th Cir. 1992).

²²⁵ *Va. State Bd. of Pharm. v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 762 (1976) (internal quotations and citations omitted).

encompasses speech that is not economically motivated, and is instead used describe the mark or to criticize it.²²⁶ This could entail social criticism, as in *Mattel v. RCA Records*.²²⁷ In *Mattel*, the Ninth Circuit held that Aqua's song "Barbie Girl," a 1990s one hit wonder, was protected speech because it was a parody on Barbie, a cultural figure.²²⁸ Similarly, nominative speech is protected because even if used in a commercial setting, the mark is merely used to designate the actual owner and is thereby deemed to be fair use.²²⁹

Use of a mark, even if used for criticism, can be problematic for trademark owners. Before the growth of the Internet, criticism was limited to small circles and did not spread rapidly throughout society.²³⁰ Cyberspace is a potentially problematic venue for trademark owners because criticism can be widely disseminated and trademark owners can thereby lose control over the reputation of their marks.²³¹ Social networking sites are even more problematic because they are heavily used and word of mouth spreads quickly on those websites.²³² In addition, by permitting everyone to use a trademark on the Internet, the mark could lose its function as a source identifier and thereby become a generic

²²⁶ See *Smith v. Walmart Stores, Inc.*, 537 F. Supp. 2d 1302, 1339–40 (N.D. Ga. 2008) (holding that defendant's use of the terms "Wal-Qaeda" and "Walocaust" constituted noncommercial speech because the defendant used the term expressively, and his economic motives were secondary at most). By definition cybersquatting is per se commercial speech. See MCCARTHY, *supra* note 12, §25:78. However, mere reservation of a website cannot constitute per se commercial speech. See *id.*

²²⁷ *Mattel, Inc. v. MCA Records, Inc.*, 296 F.3d 894, 907 (9th Cir. 2001) (discussing how Aqua's song, "Barbie Girl" criticized the source).

²²⁸ *Id.*

²²⁹ See *New Kids on the Block*, 971 F.2d at 308–09. Such speech would include a comparison made in an advertisement to differentiate or situate one's brand in the market. *Id.*

²³⁰ See McGeeveran, *Disclosure*, *supra* note 98, at 1122–27.

²³¹ See *id.* Indeed, this was the case with the fake BP account on Twitter. See Stelter, *supra* note 27.

²³² See generally Stelter, *supra* note 26 (discussing how within the span of months, 145,000 followers began to follow the fake BP profile, which produced damaging tweets).

term.²³³ Therefore, it is understandable why trademark owners would want to control discussion and use of the mark on social media websites.

The problem that arises from the enforcement of trademark rights is that the high cost of litigation will discourage users from expressing themselves in a social setting.²³⁴ In *Smith v. Walmart Stores, Inc.*, a clear case of fair use, Walmart flooded the court with expert evidence and prolonged the trial for two years.²³⁵ Indeed after receiving an ample amount of evidence, the court engaged in a lengthy likelihood of confusion analysis.²³⁶ A likelihood of confusion analysis requires significant evidence, specifically the use of expensive experts,²³⁷ and the length of a likelihood of confusion trial could result in expensive legal fees.²³⁸ In the social media context, large and expensive law firms are already encouraging trademark owners to preemptively enforce their proprietary interests with regards to username infringement.²³⁹ The threat of litigation could stifle expression through creative usernames.²⁴⁰ If courts grant trademark owners a monopoly over a mark, it could inhibit expression because users simply would not want to risk being sued for trademark infringement.²⁴¹

A remedy for this problem, advocated by Professor Bill McGeveran, would be to weed out the obvious free speech

²³³ See McGeveran, *Disclosure*, *supra* note 98, at 1144–1145.

²³⁴ See McGeveran, *Rethinking Trademark Fair Use*, *supra* note 223, at 52.

²³⁵ See *Smith v. Walmart Stores, Inc.*, 537 F. Supp. 2d 1302, 1339–40 (N.D. Ga. 2008)

²³⁶ See *id.*

²³⁷ See *id.*

²³⁸ See McGeveran, *Rethinking Trademark Fair Use*, *supra* note 223, at 99.

²³⁹ See, e.g., Lynn Humphreys, *Protecting Your Trademark From Facebook Username Abuse*, MORRISON & FOERSTER (June 11, 2009), <http://www.mofo.com/news/updates/files/15669.html>.

²⁴⁰ See *id.* There is also the risk that judges won't understand the humor in a parody or in criticism. See generally *Anheuser-Busch v. Balducci*, 28 F.3d 769 (8th Cir. 1994). In *Balducci*, the plaintiff's parody ("Michelob Oily") was not protected speech because the defendant used the Michelob mark as a weapon to criticize dependence on oil, not the source. *Id.* at 774–77.

²⁴¹ See McGeveran, *Rethinking Trademark Fair Use*, *supra* note 223, at 51–66.

cases.²⁴² If a username is used for criticism of the source, nominative use, or non-commercial fair use, then courts should dismiss the case.²⁴³ Rather than raising this affirmative defense after going through the prima facie elements for confusion, defendants should be able to raise this argument before going through the test.²⁴⁴ Litigation is costly and burdensome for defendants, and by shortening litigation, users would still be able to use words to express themselves without seriously infringing a mark.

IV. POLICY PRESCRIPTIONS FOR CYBERSQUATTING ON SOCIAL MEDIA WEBSITES

The advent of username features on social networks could be much more than a nuisance to trademark owners if it poses a grave threat to their proprietary interests. If trademark owners do not enforce their rights in this realm, they will face the risk of genericide or dilution of their brand name.²⁴⁵ Users could post vulgar updates that would taint the reputation of the mark. There is also the potential of consumer confusion.²⁴⁶ If social media websites tolerate such genericide or dilution, it would result in a diminished potency of the brand name's power in electronic commerce.²⁴⁷ Therefore, the loopholes in both the ACPA and in these websites' policies need to be addressed to provide trademark owners with adequate protection.²⁴⁸

²⁴² *Id.* at 122.

²⁴³ *Id.*

²⁴⁴ *Id.*

²⁴⁵ Darrow & Ferrera, *supra* note 54.

²⁴⁶ See McGeeveran, *Disclosure*, *supra* note 98, at 1144–45.

²⁴⁷ See *Nestle Co., Inc. v. Chester's Market, Inc.*, 571 F. Supp. 763, 766–68 (D. Conn. 1983) (discussing marks that lose the power to identify the source and holding that the term “Toll House” lost its ability to identify Nestle as the source of the mark).

²⁴⁸ See Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1125(d)(1)(B)(i)(II) (West 2006) (establishing the legal name safe harbor); *Id.* at § 1125(d)(1)(B)(ii) (establishing the “reasonable belief” safe harbor).

A. Remedies for Common Law Doctrine and the ACPA

Since Congress did not foresee increased user control on the Internet, the ACPA is outdated and could potentially be deemed to be inapplicable in this venue. Therefore, Congress needs to clarify and amend certain provisions within the statute.

First, metatag infringement should be separated from the Lanham Act. Trademark infringement on social media sites is not limited to username infringement. The ACPA would not reach these “hashtags” because social media sites do not control or assign the use of such search items.²⁴⁹ On the one hand, the infringing use of a metatag is not quite as harmful as it was in the days of *Brookfield*, as Internet users are not the luddites that courts assumed they were in the 1990s.²⁵⁰ Even so, the damage could be fairly far reaching, possibly even leading to genericide of the mark.²⁵¹ Such tags would draw consumers to impostor profiles, confuse consumers, and weaken the brand’s power.²⁵² The reason for creating a separate cause of action is that metatags are not a good fit for either the ACPA or the Lanham Act. While these search terms do not have the preclusive effect of cybersquatting, they traffic Internet users to another site and in doing so, harm the trademark owner.²⁵³

Courts examine these search items under the standard eight factor likelihood of confusion analysis,²⁵⁴ rather than employ the

²⁴⁹ See 15 U.S.C.A. § 1127 (defining domain name as one which is assigned by a registrar); *What are Hashtags (# Symbols)?*, TWITTER HELP CENTER, <http://support.twitter.com/articles/49309-what-are-hashtags-symbols> (last visited Oct. 15, 2010).

²⁵⁰ See *GoTo.com, Inc. v. Walt Disney Co.*, 202 F.3d 1199, 1209 (9th Cir. 2000) (“[E]ven modern-day Luddites are now capable of navigating cyberspace.”).

²⁵¹ See Darrow & Ferrera, *supra* note 54.

²⁵² See *Faegre & Benson, LLP v. Purdy*, 367 F. Supp. 2d 1238, 1246–47 (D. Minn. 2005) (enjoining the defendant from future use of the plaintiff’s marks in metatags that could misdirect consumers to an infringing website).

²⁵³ MCCARTHY, *supra* note 12, §25:69.

²⁵⁴ *N.Y. State Soc’y of Certified Pub. Accountants v. Eric Louis*, 79 F.Supp.2d 331, 340 (S.D.N.Y. 1999) (examining the metatag infringement under the *Polaroid* analysis).

condensed analysis articulated in *GoTo.com v. Walt Disney*.²⁵⁵ Indeed, a judge would be hard-pressed to find that many of the eight factors are applicable on the Internet.²⁵⁶ Courts should depart from the eight factor analysis for metatag infringement because it is too difficult of a standard to pass,²⁵⁷ and instead should follow the two factor analysis under *GoTo.com*.²⁵⁸

Second, Congress needs to clarify the ACPA's bad faith provision. The ACPA creates a safe harbor for a registrant who registers a name "that is otherwise commonly used to identify that person."²⁵⁹ Registration of such a name, which could include nicknames, would help to establish that the user did not register a domain name in bad faith.²⁶⁰ In the social media setting, scrutinizing whether the username was reserved in bad faith would be problematic because essentially all of the infringers would claim that the username is their nickname.²⁶¹ In some cases, ascertaining whether the nickname was registered in bad faith would be easy, as the reservation of the username in such cases would satisfy many of the non-exclusive factors set forth in the ACPA.²⁶² In other cases, the user might register a username in good faith not knowing of the similarity between his nickname and the trademark.²⁶³ Congress could clarify the provision by providing evidentiary standards to quickly and easily ascertain if the user reserved the username in good faith.

Finally, Congress should harmonize the ACPA with Section 230 of the CDA. The problem with Internet cases is that virtually

²⁵⁵ See *GoTo.com, Inc.*, 202 F.3d at 1206–07.

²⁵⁶ See *id.*

²⁵⁷ See, e.g., *Bihari v. Gross*, 119 F. Supp. 2d 309, 318–19 (S.D.N.Y. 2000) (finding that the abusive use of metatags did not create a likelihood of confusion).

²⁵⁸ See *GoTo.com, Inc.*, 202 F.3d 1206–07.

²⁵⁹ Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1125(d)(1)(B)(i)(II) (West 2006).

²⁶⁰ See *infra* Part II.C.2.

²⁶¹ *CNN L.P. v. CNNNews.com*, 177 F. Supp. 2d 506, 524 (E.D. Va. 2001)

²⁶² See *id.* (noting that the name CNN was neither the legal name, nor the name commonly used for the entity).

²⁶³ E.g., a user with a nickname "Nik E" creates a webpage at <http://myspace.com/nike>.

every trademark owner and celebrity could—and likely would—assert a cybersquatting cause of action, thus avoiding the CDA's immunity provision.²⁶⁴ Allowing such claims could flood the courts with baseless secondary liability claims and could become burdensome for social media sites as well. Congress should weaken the express exemption for intellectual property claims under Section 230(e) of the CDA because that section completely eliminates immunity for any intellectual property cause of action.²⁶⁵ While this discourages ISPs from ignoring trademark infringement, it also subjects ISPs to frivolous lawsuits. The alarming trend with Section 230(e) is that plaintiffs state a cause of action under the ACPA in order to avoid the immunity provision of CDA 230(c).²⁶⁶ Such an exemption allows plaintiffs like La Russa to state a cybersquatting claim when the claim is really predicated on defamatory status updates and profile content.²⁶⁷ By weakening this exemption, Congress could save the courts and social media websites from having to fend off frivolous lawsuits.

B. Remedies for Social Media Policy

The ACPA should not be the only remedy for this form of cybersquatting. Amending these websites' policies would provide a less costly alternative to trademark owners.²⁶⁸ Administrators of social media websites should also play an active role in curtailing such infringement. By broadening the scope of the verification mechanisms available to corporations and by enforcing the verification policy more stringently, trademark owners would be able to pursue a viable alternative to the costly litigation associated

²⁶⁴ See Macmillan, *supra* note 24 (noting the distinction between trademark infringement and protections afforded ISPs under Section 230 in cases dealing with celebrities).

²⁶⁵ Communications Decency Act, 47 U.S.C.A. § 230(e)(2) (West 2006).

²⁶⁶ See, e.g., Mike Masnick, *And Here Come the Youtube Copyright Lawsuits*, TECHDIRT.COM (Jul. 17, 2006, 6:54 PM), <http://www.techdirt.com/articles/20060717/1852217.shtml> (examining how individuals suing Youtube were attempting to avoid immunity under the CDA by invoking a new ruling in which file sharing networks could be held liable for copyright infringement).

²⁶⁷ See Macmillan, *supra* note 24.

²⁶⁸ See *supra* Part III.A.

with the ACPA.²⁶⁹ Moreover, these administrators would serve as gatekeepers and weed out unnecessary and frivolous litigation.

1. Verification Features

Verification features are useful tools to proactively combat username infringement. Both Twitter and Facebook have such features, but both need to be amended in order to provide trademark owners with adequate protection. Strengthening these features will allow Twitter's and Facebook's trademark policies to be proactive rather than retroactive. Twitter has become a haven for cybersquatters and therefore needs to amend its current verification policy. Twitter should extend its verification feature to include all corporations. Currently, the policy only applies to some large conglomerates, such as Target.²⁷⁰ Twitter is currently testing a verification policy for businesses, but the website is not accepting verification requests from all businesses yet.²⁷¹ Under the current Twitter verification policy, users are free to pose as corporations and free ride off the good will of that corporation.²⁷² Evidence of reservation of famous brands as usernames suggests that this is exactly what is happening on Twitter.²⁷³ Permitting such free riding could lead to genericide of the mark, tarnishment of the owner's reputation, and consumer confusion. Expansion of the verification tool to all corporations would help to curtail cybersquatting on Twitter because the verification badge allows users to discern the official profile for each corporation and its brand names.²⁷⁴ The verification tool would also cut consumer search costs because a user would be able to spot a fake profile, even if they were misled by a deceptive hashtag.²⁷⁵ In doing so, this would also protect the consumer from fraud.

Facebook's policy may also need to be amended. Although

²⁶⁹ *Id.*

²⁷⁰ *See supra* notes 132–134 and accompanying text.

²⁷¹ *Business Verification*, TWITTER, *supra* note 132.

²⁷² *See id.*

²⁷³ *Wee*, *supra* note 135 (discussing the abusive reservation of usernames such as Pringles, Apple, and Dell).

²⁷⁴ *See infra* Part II.B.

²⁷⁵ *See id.*

Facebook does have a verification feature, it appears to be a weak one. Currently, Facebook requires that an official representative reserve the username and the administrators verify such accounts via mobile authentication.²⁷⁶ Impostors could pose as official representatives and pose as the representative during “mobile authentication.”²⁷⁷ As a solution, the representative should be required to produce proof of ownership of the mark; a registration certificate, for example, would be sufficient proof here. The website should also require verification through a company email address. A more stringent implementation of the verification policy would help circumvent the problem and discourage impostors from trying to verify their profiles fraudulently.

In addition, Facebook’s verification policy does little to avoid consumer confusion. Specifically, the verification²⁷⁸ feature does not feature a visual “badge” like Twitter’s verification feature.²⁷⁹ By creating a badge for verified accounts, users would easily be able to discern fake profiles from real ones. Creating these badges would therefore reduce search costs and reduce the potential harms of username infringement.

2. Reporting Procedures: A Method to Avoid Costly Litigation

Trademark owners would be wise to work with the administrators of social media sites to shut down impostor profiles. Both Facebook and Twitter encourage trademark owners to report instances of name squatting.²⁸⁰ Both websites require the trademark owner to provide proof of ownership via a registration number.²⁸¹ Since protection is predicated on registration of the

²⁷⁶ See *id.*

²⁷⁷ *Id.*

²⁷⁸ See O’Neill, *supra* note 102.

²⁷⁹ See *Business Verification*, TWITTER, *supra* note 132.

²⁸⁰ *Report an Infringing Username*, FACEBOOK, http://www.facebook.com/help/contact.php?show_form=username_infringement (last visited Sept. 10, 2010); *Trademark Policy*, TWITTER, <http://support.twitter.com/articles/18367-trademark-policy> (last visited Sept. 10, 2010).

²⁸¹ *Report an Infringing Username*, FACEBOOK, *supra* note 281; *Trademark Policy*, TWITTER, *supra* note 153. It seems as though only registered marks will be protected here. It is not clear whether unregistered mark owners would be

mark, the brand owner would be wise to register his mark or risk losing the benefits of the reporting mechanisms.²⁸² Significantly, this process is relatively inexpensive in comparison to litigating against the mark owner.²⁸³ The mark owner would also get what he wants—the username would be transferred and the impostor profile will be shut down.²⁸⁴

Moreover, the administrators would be able to weed out frivolous complaints, particularly where there is a free speech interest at stake. For example, if a username is “Nikesucks” or any other form of clear criticism, the administrators should dismiss any related complaints because this is clearly a form of criticism with the source as the target.²⁸⁵ Employing this strategy will create an alternative to costly litigation by working constructively with the administrators of social media websites.

In some cases, specifically with unregistered marks, litigation might be inevitable.²⁸⁶ Site administrators might refuse to transfer or eliminate the infringing profile; in such a case, the plaintiff would be forced to appeal. In this event, litigation would be necessary to protect the mark owners’ interests.²⁸⁷ Consequently, the plaintiff should only litigate when the social media site

able to profit from this form.

²⁸² *Facebook URLs—Trademark Piracy Shoals Ahead*, THE ORANGE RAG (June 12, 2009, 07:21 BST), http://www.theorangerag.com/blog/_archives/2009/6/12/4219264.html (discussing how the Facebook username form is not applicable to unregistered trademarks and encouraging users to register brand names).

²⁸³ See McGeeveran, *Rethinking Trademark Fair Use*, *supra* note 223, at 70.

²⁸⁴ *Report an Infringing Username*, FACEBOOK, *supra* note 281 (providing an option for the trademark owner to request a transfer of the username).

²⁸⁵ This could alleviate the problem of burdensome litigation that McGeeveran examined in *Rethinking Fair Use*. See generally McGeeveran, *Rethinking Trademark Fair Use*, *supra* note 223. Rather than have the court serve as the gatekeeper for these frivolous claims, administrators could weed out the claims that are obviously protected by fair use and the court should respect those decisions.

²⁸⁶ See Charles Christian, *Facebook URLs—Trademark Piracy Shoals Ahead*, LEGAL TECHNOLOGY INSIDER (June 12, 2009, 7:29 PM), http://www.theorangerag.com/blog/_archives/2009/6/12/4219264.html (discussing how the username form is not applicable to unregistered trademarks).

²⁸⁷ See *id.*

wrongly rejects his complaint and such litigation should be a last resort because it is expensive and time consuming. In sum, plaintiffs, and even defendants, should use litigation when there are no other alternatives available.

CONCLUSION

Cybersquatting on social media websites poses to trademark owners a real threat that must be addressed. Trademark owners should not immediately pursue a cause of action under the ACPA. Instead, trademark owners should work with these websites to protect their own interests. Trademark owners have a number of options at their disposal—they could: (1) ask the website to transfer the username, (2) ask the website to shut down the profile or hashtag, (3) contact the profile owner and ask him to transfer the username, or (4) verify the account.²⁸⁸ To create a viable option for creating an official page, web administrators need to create a strong verification policy to proactively combat name squatting. Doing so will prevent serious damage to a trademark.

These policy problems are not confined to social media websites. The ACPA is an outdated statute, one which needs to be amended to adequately address the modern and complex issues associated with cybersquatting on social media websites. Congress should amend the bad faith provision, particularly its safe harbor provision. In addition, Congress needs to weaken the CDA's exemption of intellectual property claims from its immunity provision to prevent frivolous litigation. It is crucial that such changes are made in order to prevent cybersquatters from getting a free ride from a mark and to protect the brand of mark owners on social media websites.

²⁸⁸ *Cybersquatting the Social Networks: A New Trademark Risk*, TRAVERSELEGAL (Apr. 23, 2009, 11:45 AM), <http://tcattorney.typepad.com/domainnamedispute/2009/04/cybersquatting-the-social-networks-a-new-trademark-risk.html#more>.