NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 17, ISSUE 1: OCTOBER 2015

SHOULD CONTRIBUTORY CYBERSQUATTING BE ACTIONABLE?

Nicholas Foss Barbantonis *

Domain name registrars are increasingly targeted by trademark owners for registering and hosting infringing domain names, despite the lack of clear statutory authorization for these claims. Registrars, pressed by reduced profit margins, have begun offering value-added services such as sponsored domain parking and WHOIS-masking. However, such services incentivize and aid domain name purchasers to engage in infringement. Existing scholarship on secondary liability in trademark law and cybersquatting is scarce and outdated. This Article provides a theoretical approach to the question of whether, and when, contributory cybersquatting liability exists. The Article argues that the relevant statute, the Anticybersquatting Consumer Protection Act (ACPA), was enacted against the backdrop of judicial precedent and Congressional intent to enhance trademark enforcement. By drawing upon the substantial case law undergirding traditional contributory trademark infringement, the Article contends that the motivations for including secondary liability apply to ACPA as well.

---

* Nicholas Foss Barbantonis (LL.M., University of Oslo 2013, LL.M., Michigan State University College of Law 2013), Doctor of Juridical Science (SJD) Candidate 2016; University of Arizona James E. Rogers College of Law. I especially thank my dissertation committee supervisor Professor Derek Bambauer for his invaluable thoughts on the topic and insightful comments on this article. I also thank Professor Adam Candeub for bringing this issue to my attention, and Professors Sean A. Pager, Jennifer Carter-Johnson and David Gantz for their continuing support. I also thank my good friend Eric Rogers for his comments on an earlier draft. Comments are welcomed at <nfb@email.arizona.edu>. All mistakes and omissions are my own.

TABLE OF CONTENTS

I. INTRODUCTION

There is an ongoing controversy as to whether the Anticybersquatting Consumer Protection Act (ACPA) includes a cause of action for contributory cybersquatting for domain name registrars.[1] Contributory cybersquatting's basic mechanism entails an action to pursue cybersquatting caused by a third party's bad faith domain registration and subsequent use of another's mark. It is not the registrant (or the primary infringer) of the domain name who is challenged. Instead, it is the domain name registrar. The assertion of contributory liability is especially incentivized in the realm of Internet domain names.[2] Given that the registrars accounting for the majority of domain name registrations are multi-million dollar corporations, judgments against registrars, contrary to those against individual defendants, will also be easier to enforce.[3]

Several earlier district court decisions have held both implicitly and explicitly that such an action is available.[4] However, the situation took a dramatic turn in *Petroliam Nasional Berhad v.*

---

[1] *See* 15 U.S.C. § 1125(d) (2012). A registrar is responsible for maintaining the registry, and is the actor that potential purchasers of domain names (registrants) contacts to reserve domain names. Examples of major registrars are Godaddy.com and domain.com.

[2] This is because the potential efficiency of pursuing relief by a domain name registrar is much greater since they are generally easier to locate. This is discussed further *infra* Part II.D.

[3] Michael J. De La Merced, *As I.P.O. Nears, GoDaddy Tries to Show It's More Than Just Domain Names*, N.Y. TIMES (Aug. 14, 2014), http://dealbook.nytimes.com/2014/08/14/as-i-p-o-nears-godaddy-tries-to-show-its-more-than-just-domain-names/?_php=true&_type=blogs&_r=0 (finding that GoDaddy.com, one of the leading registrars, reported $658.7 million in revenue for the first six months of 2014).

[4] *E.g.*, Ford Motor Co. v. Greatdomains.Com, Inc., 177 F. Supp. 2d 635 (E.D. Mich. 2001); Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092 (C.D. Cal. 2009); Microsoft Corp. v. Shah, No. C10-0653 RSM, 2011 WL 108954 (W.D. Wash. Jan. 12, 2011); Verizon Cal., Inc. v. Above.com Pty, Ltd., 881 F. Supp. 2d 1173 (C.D. Cal. 2011).

GoDaddy.com, Inc.,[5] in which the Ninth Circuit Court of Appeals concluded the opposite—the cause of action does not exist.[6]

The issue regarding the actionability of contributory cybersquatting liability is not new. The issue has, however, become more critical as a result of the ever-changing registrar market conditions. This is especially true when considering the historical surge in domain name registrations and the prognosis of an ever-increasing poll of new top-level domain names (TLD) introduced by the Internet Corporation for Assigned Names and Numbers (ICANN).[7] Although the domain registration business is a multi-billion dollar industry, profit margins are shrinking due to fierce competition among the registrars.[8] In order to maximize profit, several registrars have started to offer services outside of the core functions—registering and maintaining domain names. This Article focuses on registrar services such as sponsored domain parking and WHOIS-masking.[9] Both services are generally considered to be outside of registrar functions such as registering and maintaining domain names. Insightful scholarship is scarce

[5] 737 F.3d 546 (9th Cir. 2013), *cert. denied*, No. 13-1255, 2014 WL 1496428 (U.S. Oct. 6, 2014).

[6] *Id.* at 548.

[7] *What Does ICANN Do?*, ICANN, https://www.icann.org/resources/pages/what-2012-02-25-en (last visited Aug.17, 2015); *see New Generic Top-Level Domains Announcements*, ICANN, http://newgtlds.icann.org/en/announcements-and-media/latest (last visited Aug. 17, 2015).

[8] *VeriSign's Renewal Rates Improve For Q2 2015*, TREFIS (July 24, 2015), http://www.trefis.com/stock/vrsn/articles/307215/verisigns-renewal-rates-improve-for-q2-2015-while-it-plans-rollout-of-new-idns-and-a-fresh-round-of-price-hike-for-net/2015-07-24; Brian Wu, *GoDaddy Stock: GDDY Is Growing Like a Weed, But . . .* , INVESTORPLACE (Aug. 6, 2015), http://investorplace.com/2015/08/godaddy-stock-gddy-is-growing-like-a-weed-but/#.VdHuErKqpBc.

[9] *See infra* Part II.B for an explanation of the services. Although several other services exist with categories arguably outside of "core functions," this Article will primarily focus on the services: domain parking and WHOIS-masking.

and primarily deals with the outdated juridical landscape prior to the Ninth Circuit *Petroliam* decision.[10]

This Article seeks to revisit the prior decisions and investigate whether contributory cybersquatting is constitutional. Although the Ninth Circuit is a heavy authority on intellectual property law, it is important to remember that the United States Supreme Court has never discussed the issue. This Article concludes that there should be a cause of action for contributory cybersquatting for domain name registrars.

II. BACKGROUND

A. *The Internet*

The International Telecommunication Union reports that the Internet currently has 3.2 billion users—about 44% of the total world population.[11] There are currently a staggering 294 million active TLD registrations.[12] Registrations have increased by 6.6% in the past years,[13] making evident the domain names' value and ever-increasing integral part of modern business and social life. Few could have anticipated such immense development. The considerable registration statistics do, however, have a backside. Indeed, it increases the potential for dispute between mark owners and cybersquatters. It all started in the mid-1980s when scientists

---

[10] Christine A. Walczak, *The New and Evolving Tort of Contributory Cybersquatting: Did the Courts Get It Right?*, 2012 U. ILL. J.L. TECH. & POL'Y 531 (2012) (discussing why contributory cybersquatting has no statutory basis and as such is not actionable); Kurt M. Saunders, *Is Contributory Cybersquatting the Next Front in Domain Name Litigation?*, PENN. B. ASS'N, INTELL. PROP. L. NEWSL., Spring 2011; Darryl C. Wilson, *Battle Galactica: Recent Advances and Retreats in the Struggle for the Preservation of Trademark Rights on the Internet*, 12 J. HIGH TECH. L. 1, 23–24 (2011); Advising e Bus. § 6:49.

[11] *ICT Facts & Figures*, ICT, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (last visited Sept. 1, 2015).

[12] The Domain Name Industry Brief, VERISIGN, Vol. 12, Issue 2, June 2015, *available at* https://www.verisign.com/assets/domain-name-report-june2015.pdf.

[13] *Id.*

developed the Internet Protocol Suite ("TCP/IP"), which allowed computers to communicate across networks over vast geographical distances.[14] With the implementation of TCP/IP, every computer connected to the network now had a unique, either statically or dynamically, Internet Protocol ("IP") address.[15]

For communication to flow between two or more computers, one needs to know the recipient's IP address. The vast majority of servers visited by regular web-surfers have an assigned static IP address. This system is very similar to our current telephone system. As most individuals born before the 1990s can recall, it may be cumbersome to remember or bookmark every IP address. It is also challenging for corporations to market a particular brand through an IP address. This is further complicated by the fact that a given website IP may change for various reasons including switching between hosting companies. Corporations with large online presence, such as Google.com, Facebook.com, etc., cannot rely on a single server, however powerful, as it will not able to process all requests simultaneously. This issue is exacerbated by larger distances and increasing latency, inhibiting the consumers' experience.

To counter these issues, enterprises utilize a system that links several hundred servers all over the world to balance server load and delay. This would not have been practically possible without the Domain Name System ("DNS"). A DNS attaches a domain name to IP addresses. This gives two great advantages: the user no

---

[14] Barry M. Leiner et al., *Brief History of the Internet, Internet Society*, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Feb. 1, 2015).

[15] The current main protocol, which is called IPv4, is an address containing a series of four numbers separated by decimals, i.e. 100.101.201.1. Initially the circa 4.3 billion addresses under the IPv4 (32-bit numeric address), which during its infancy seemed like a generous amount, are actually starting to run out. To counter this, the new IPv6 (128-bit hexadecimal numeric address), is currently being rolled out. In comparison, the new protocol has 2^{128}, or circa 340 trillion combinations. An IPv6 address looks like this: 3ffe:1900:4535:2:200:f8ff:fe21:57cf.

longer needs to know the IP address; and the host is no longer bound by a single IP address—it can simply update the connected IP addresses to the domain name. In today's society, being readily available on the Internet is invaluable to any business. However, as will be discussed below, the advent of the domain name has also created the issue of people utilizing domain names that are similar to the trademarks of recognizable businesses with the aim of making an easy profit and owners of various marks ("cybersquatting").

B. *Cyberpiracy*

Cyberpiracy is an umbrella term primarily covering cybersquatting and typosquatting. Cybersquatting is "the bad faith registration of domain names with intent to profit from the goodwill associated with the trademarks of another."[16] Traditionally, a cybersquatter would speculate by wrongfully registering several domains in the hope that they could receive a larger sum from the true mark holder to gain ownership of it. Typosquatting is a newer phenomenon, where the registrant registers multiple domains that misspell various marks in the hope that unknowing web surfers will enter their sites and generate traffic, either to sell their own infringing products or to front various advertisements of third party competing or infringing products and earn a given amount per click accumulated.[17] An example of typosquatting would be aple.com, instead of apple.com. For both types of cyberpiracy, squatters have been found to misuse the marks' accumulated goodwill by diluting or tarnishing the mark by redirecting traffic to sites selling infringing goods or services and adult or obscene third party websites. In any case, the mere act of denying the trademark owner use of the

[16] Vulcan Golf, LLC v. Google Inc., 726 F. Supp. 2d 911, 915 (N.D. Ill. 2010) (quoting Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1099 (C.D. Cal. 2009)).

[17] Christopher G. Clark, *The Truth in Domain Names Act of 2003 and A Preventative Measure to Combat Typosquatting*, 89 CORNELL L. REV. 1476, 1488 (2004).

domain name in today's society of e-trading may seriously impact the rightful owner's ability to succeed.

The ACPA, which was passed as an amendment to the Lanham Act in 1999,[18] protects U.S. marks that are either registered with the United States Patent and Trademark Office ("USPTO"), or that are distinctive or famous.[19] The statute requires the plaintiff to prove the domain name is identical or confusingly similar (dilution) and that the registrant has the "bad faith intent to profit from that mark."[20] The statute seeks to minimize shortcomings of the Lanham Act's general trademark provisions, which requires the infringing use to be "in commerce."[21] The ACPA also intended to explain the shortcomings of the Federal Trademark Dilution Act ("FTDA"), which one commentator argued was a "circus among the circuits" as some circuits required marks to be nationally renowned, while some only required niche market fame, and some required actual dilutive harm.[22] In 2003, the Supreme Court in *Mosely v. V Secret Catalogue, Inc.* held that there was a requirement of actual confusion.[23] *Moseley* was finally superseded in 2006 by the Trademark Dilution Revision Act ("TDRA"), which amended the Lanham Act to require only a likelihood of confusion.[24]

To vindicate a claim under the ACPA, it is no longer required that the mark be both distinctive and famous to be protected.[25] The

---

[18] 15 U.S.C. § 1051 et seq. (2012).

[19] *Id.* § 1125(d)(1)(A) (Both unregistered distinctive and famous marks are protected when considered recognized common law marks.).

[20] *Id.* § 1125(d)(1)(A)(i).

[21] *Id.* § 1114(1)(a).

[22] Xuan-Thao N. Nguyen, *Blame It On the Cybersquatters: How Congress Partially Ends the Circus Among the Circuits with the Anticybersquatting Consumer Protection Act*, 32 LOY. U. CHI. L.J., 777, 777–813 (2001).

[23] Moseley v. V Secret Catalogue, Inc., 537 U.S. 418 (2003).

[24] Trademark Dilution Revision Act Of 2006, Pub. L. No 109–312, 120 Stat. 1730 (2006).

[25] In 15 U.S.C. § 1125(d)(1)(A), the statute states:

> [W]ithout regard to the goods or services of the parties that person—
> (i) has a bad faith intent to profit from . . . [a] mark . . . ; and

plaintiff is also not required to show actual dilution or a likelihood of dilution.[26] Instead, the ACPA's main function is to protect against "bad faith intent to profit."[27] When determining "bad faith," the statute lists a non-exclusive nine-factor list:

> (I) the trademark or other intellectual property rights of the person, if any, in the domain name;
>
> (II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
>
> (III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
>
> (IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
>
> (V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
>
> (VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
>
> (VII) the person's provision of material 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;

> (ii) registers, traffics in, or uses a domain name that—
>
> (I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
>
> (II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or
>
> (III) is a trademark, word, or name protected by reason of section 706 of title 18 [the Red Cross] or section 220506 of title 36 [the Olympics].

[26] *Id.*

[27] *Id.*

> (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 [Dilution by blurring; dilution by tarnishment].[28]

The factors fall in two groups in which the first four suggest a lack of bad faith, and the last five are indicia of bad faith intent.[29] Not being able to find goodwill is not necessarily an indication of bad faith, and finding goodwill is not necessarily an indication of the opposite.[30] The statute also has a safe harbor, which limits liability where "the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful."[31]

Mark owners often face the challenge of a person registering identical or confusingly similar domain names. Excluding the hardship of regular trademark litigation, the challenge is two-fold. First, locating the registrant can be challenging because the database containing information about the registrants of domain names, the WHOIS records,[32] is often masked. A "masked" WHOIS is usually a legitimate registration by a proxy acting as an agent for the registrant to preserve the registrants' anonymity

---

[28] *Id.* § 1125(d)(1)(B)(i).

[29] H.R. REP. 106-412 at 10 (1999); Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 489, 498 (2d Cir. 2000) ("[W]e are not limited to considering just the listed factors when making our determination of whether the statutory criterion has been met. The factors are, instead, expressly described as indicia that 'may' be considered along with other facts.").

[30] S. REP. 106-140 at 8 (1999).

[31] 15 U.S.C. § 1125(d)(1)(B)(ii).

[32] WHOIS is a searchable database that lists all current domain name registrations. The database contains information such as the registrants' contact information, and the date of registration and expiration.

against spam. GoDaddy.com is one of many registrars that offer this service. They will register the registrant's information on a confidential database and put generic information on the public WHOIS database.[33] GoDaddy.com now requires third parties to provide affidavits or court orders to reveal the registrant's real information.[34] The WHOIS records are also often inaccurate, because registrars are not obligated to investigate the truthfulness of registrants' information when receiving applications for domain names. Although some registrars implement so-called "click-wrap" terms of service requiring the registrant "to keep . . . [the WHOIS] information in a current and accurate status",[35] the practical reality is that it is sufficient to provide falsified information such as name, telephone number, and address along with a valid credit card number, which anyone can buy anonymously. This gives cybersquatters the opportunity to provide false information and hide their identities.

Second, owners of famous marks in particular are prone to cybersquatting from multiple squatters who each register several domain names. Such scenarios force plaintiffs to file multiple suits against several different cybersquatters. This is both time-consuming and expensive.

C. *Secondary Liability*

The Lanham Act does not expressly mention secondary liability for trademark infringement.[36] Secondary liability comprises both participant-based and relationship-based liability

---

[33] *See* GoDaddy.com, https://www.godaddy.com/domainaddon/private-registration.aspx?ci=92976 (last visited Apr. 10, 2015) (offering WHOIS masking for an annual fee of $7.99 per year per registered domain name).

[34] *See GoDaddy.com's Domain Name Proxy Agreement*, http://www.godaddy.com/agreements/showdoc.aspx?pageid=DOMAIN_NAME PROXY (last visited Apr. 10, 2015).

[35] *See GoDaddy.com Domain Name Registration Agreement*, https://www.godaddy.com/agreements/showdoc.aspx?pageid=REG_SA&isc=cjc1hos1 (last visited Oct. 10, 2014).

[36] *See* 15 U.S.C. § 1125 (2012).

and is a purely court-created doctrine based on principles of secondary liability in tort cases.[37]

Participant-based infringement refers to conduct in which the primary infringer's injurious behavior is induced, contributed to, or facilitated by a secondary infringer.[38] The main aspect of such claims is usually tied to the secondary infringer's knowledge or lack thereof, and to the level of active harmful contribution.[39] Relationship-based liability is based on the principle of *respondeat superior* and focuses on the defendant's control and accrued benefits due to the harm caused by the primary infringer.[40] If the relationship between the defendants is close enough, courts will treat them as one.[41] This Article will focus on participant-based liability, also known as contributory liability.

The landmark case for contributory infringement liability is *Inwood v. Ives*.[42] The case involved a generic drug, which the

---

[37] *See* Inwood Labs. Inc. v. Ives Labs., Inc., 456 U.S. 844 (1982).

[38] *See* Graeme B. Dinwoodie, *Secondary Liability for Online Trademark Infringement: The International Landscape*, 37 COLUM. J.L. & ARTS 463, 463 (2014).

[39] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 26 (1995) (stating "(1) One who, on behalf of a third person, reproduces or imitates the trademark, trade name, collective mark, or certification mark of another on goods, labels, packaging, advertisements, or other materials that are used by the third person in a manner that subjects the third person to liability to the other for infringement under the rule stated in § 20 is subject to liability to that other for contributory infringement; (2) If an actor subject to contributory liability under the rule stated in Subsection (1) acted without knowledge that the reproduction or imitation was intended by the third person to confuse or deceive, the actor is subject only to appropriate injunctive relief.").

[40] Dinwoodie, *supra* note 38; Procter & Gamble Co. v. Haugen, 317 F.3d 1121 (10th Cir. 2003).

[41] Hard Rock Cafe Licensing Corp. v. Concession Services., Inc., 955 F.2d 1143, 1150 (7th Cir. 1992) (stating vicarious liability requires the infringer and defendant to have "apparent or actual partnership" and to have "authority to bind one another in transactions with third parties or exercise joint ownership or control over the infringing product").

[42] 456 U.S. 844 (1982).

defendant manufacturer sold through third party pharmacists.[43] While some of the pharmacists committed primary infringement by selling the drug as the branded version, the plaintiff chose to pursue the generic drug manufacturer for contributory infringement.[44] The U.S. Supreme Court held that:

> [I]f a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorially responsible for any harm done as a result of the deceit.[45]

The *Inwood* test is two-fold. First, one must find intentional inducement, and second, one must find a continued supply of the product, which the petitioners knew were infringing.[46] The first prong is relatively uncomplicated as it simply includes an analysis of whether or not there is intentional infringement. The second prong, however, is less obvious. The second prong was elaborated in *Hard Rock Café Licensing Corp. v. Concession Services, Inc.*[47] The case involved counterfeit Hard Rock Café t-shirts, sold by various vendors at a flea market, and whether the flea market could be held contributorily liable for allowing such practice.[48] The court's conclusion was that the flea market could be held liable if "willfully blind" to the trademark infringement conducted by the vendors.[49] The court explained that "[i]n the absence of any suggestion that a trademark violation should not be treated as a common law tort" the flea market was "responsible for the torts of those it permits on its premises."[50] The question becomes whether

---

[43] *Id.*
[44] *Id.* at 849.
[45] *Id.* at 854.
[46] *Id.* at 855.
[47] 955 F.2d 1143, 1148–49 (7th Cir. 1992).
[48] *Id.* at 1145–46.
[49] *Id.* at 1149.
[50] *Id*.

the owner of the premises "know[s] or ha[s] reason to know that the other is acting or will act tortiously."[51]

The flea market analysis was further expanded in *Lockheed Martin Corp. v. Network Solutions, Inc.*[52] to also include services. The question then becomes whether the defendant has created a marketplace where infringement occurs and the degree of control and monitoring exercised.[53] The court must also "consider the extent of control exercised by the defendant over the third party's means of infringement,"[54] and under this theory "a plaintiff must prove that the defendant had knowledge and '[d]irect control and monitoring of the instrumentality used by the third party to infringe the plaintiff's mark.'"[55]

With over twenty years of decisions finding contributory trademark infringement with no intervention by Congress, it is safe to conclude that contributory trademark infringement is settled law in the United States.[56]

D. *Secondary Liability Applied to Domain Names: Contributory Cybersquatting*

Applied to the realm of the internet, the possible advantages of secondary liability can be significant. Unlike in traditional trademark litigation where there is usually one or a few domestic

---

[51] *Id.*

[52] 194 F.3d 980 (9th Cir. 1999).

[53] *Id.* at 984.

[54] *Id.*; Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 591 F.Supp.2d 1098, 1111 (N.D. Cal. 2008).

[55] *Louis Vuitton*, 591 F.Supp.2d at 1111 (quoting *Lockheed Martin I*, 194 F.3d at 984).

[56] *See* Coach, Inc. v. Swap Shop, Inc., 916 F. Supp. 2d 1271, 1278 (S.D. Fla. 2012) (providing a clear picture of the state of the availability of contributory trademark infringement liability); *see also Inwood Labs., Inc*. 456 U.S. at 853–55; Coach, Inc. v. Gata Corp., 2011 WL 2358671, at *6 (D.N.H. June 9, 2011); Perfect 10, Inc. v. Visa Intern. Service Ass'n, 494 F.3d 788, 807 (9th Cir. 2007); Adidas America, Inc. v. Kmart Corp., 2007 WL 2915594 (D.Or. Oct. 3, 2007); *Hard Rock Cafe*, 955 F.2d at 1150; Coach, Inc. v. D & N Clothing, Inc., 2011 WL 2682969 (E.D.Mich. July 11, 2011).

defendants per case, the number of different registrants of similar domain names of any famous trademark might be in the hundreds and from all over the world. Registrants with masked or fake WHOIS data further complicate the matter.

The benefits of allowing secondary liability is not restricted to the direct effects of each case because it also serves as an incentive for actors such as registrars to partake more actively in the cost associated with monitoring and enforcement of infringement. That said, if both pre-screening and subsequent response to trademark notices are reasonable, registrars should not run the risk of liability.[57] There is nothing preventing registrars from conducting shallow domain and trademark searches to identify potential infringement. This may largely be automated by creating a script where the sought-after domain name is queried against national and international trademark databases. If the script detects possible infringement, it could be forwarded to a caseworker to make a preliminary determination of bad faith. Of course, this would induce an additional cost. Today's dot-com domain name prices usually hover around $10 for the first year, and between $10 and $20 for each subsequent year.[58] The price increase would likely be nominal and easily transferred to the consumers. If anything, the increased registration fee would function as an augmented threshold against cybersquatting.

It is important to note the statements above clearly contradict the ACPA's current safe harbor provision contained in § 1114(2)(D). The provision shields registrars from monetary

---

[57] Stacey L. Dogan, *Principled Standards vs. Boundless Discretion: A Tale of Two Approaches to Intermediary Trademark Liability Online*, 37 COLUM. J.L. & ARTS 503 (2014).

[58] Domain.com, https://www.domain.com (last visited Oct. 7, 2015) (showing the price to register a new dot com domain was $9.99 with a subsequent yearly price of $11.49 per year); *see also* GODADDY.COM, https://www.godaddy.com/ (last visited Oct. 7, 2015) (showing the price to register a new dot com was $2.99 per year with a minimum two year agreement with subsequent yearly price of $15 per year).

liability from certain registrar core actions.[59] As we will see below, there are multiple scenarios where the specific actions of a registrar may indeed render the provision irrelevant.[60] In clauses (ii) and (iii), the provision explicitly lists actions—including refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name in in compliance with a court order—that, if taken by the registrar would shield those entities from monetary liability.[61] The legislative history states that this was indented to "encourage[] domain name registrars and registries to work with trademark owners to prevent cybersquatting."[62]

As with traditional trademark infringement under the Lanham Act, the ACPA has no specific mention of contributory liability.[63] However, there are several cases, which deal with the theory.[64]

III. ANALYSIS OF CASES PRIOR TO PETROLIAM NASIONAL BERHAD V. GODADDY.COM

This section discusses the several district court cases leading up to the Ninth Circuit decision in *Petroliam Nasional Berhad v. GoDaddy.com*.[65]

---

[59] 15 U.S.C. § 1114(2)(D).

[60] *See e.g.*, Lockheed Martin Corp. v. Network Solutions, Inc., 141 F. Supp. 2d 648 (N.D. Tex. 2001) (stating registrars are only immunized by liability when acting as a registrar, i.e., registering domain names for registrants).

[61] 15 U.S.C. § 1114(2)(D)(i)(II) (exempting from liability "any action of refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name- (I) in compliance with a court order under section 1125(d) of this title; or (II) in the implementation of a reasonable policy by such registrar, registry, or authority prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark.").

[62] *See* S. REP. No. 106–40, at 11 (1999).

[63] 15 U.S.C. § 1051 et seq.

[64] *See supra* note 4.

[65] Petroliam Nasional Berhad v. GoDaddy.com, 737 F.3d 546 (9th Cir. 2013).

A. Ford Motor Co. v. Greatdomains.com, Inc.[66]

This case involved a defendant website, Greatdomains.com, which specialized in domain name auctions.[67] Greatdomains.com profited from commissions on sales conducted through its site.[68] The source of the controversy was a handful of domain names that included trademarks held by Ford.[69] Instead of pursuing the registrant, Ford sued Greatdomains.com for contributory cybersquatting under the flea market analysis theory, as Greatdomains.com had created the "necessary marketplace," analogous to the *Lockheed Martin Corp.* case.[70]

The court agreed that the flea market analysis *could* be applied to allegations of cybersquatting, but the court decided upon a heightened standard because, as the "ACPA requires a showing of 'bad faith intent'—a subjective element not required under traditional infringement, unfair competition, or dilution claims . . . ."[71] The U.S District Court for the Eastern District Court of Michigan concluded that it would not be sufficient for a registrar to "merely [be] aware that domain names identical or similar to protected marks were being sold over its website."[72] This is based on ACPA's safe harbor provision of non-bad faith uses, and unless the registrar "knew or should have known" of the registrants' illegitimate reasons for registering the domain in the first place, the registrar should not be held liable.[73] Thus, the court required "exceptional circumstances" for contributory liability to apply, because registrars "could not be expected to ascertain the good or bad faith intent of its vendors . . . ."[74]

---

[66] 177 F. Supp. 2d 635 (E.D. Mich. 2001).
[67] *Id.*
[68] *Id.* at 646.
[69] *Id.* at 635 (finding three domains created a high likelihood of confusion: 4fordtrucks.com, 4fordparts.com, and lincolntrucks.com).
[70] *Id.* at 646.
[71] *Id.* at 647.
[72] *Id.*
[73] *Id.*
[74] *Id.*

In *Ford Motor Co.* the court did not find "exceptional circumstances," and dismissed Ford's claim of contributory cybersquatting.[75]

B. Solid Host v. Namecheap, Inc.[76]

This case relates to a Dutch plaintiff, Solid Host, that lost control of its domain name, solidhost.com, after its registrar, eNom, had a security breach and a third party gained control of the domain and subsequently moved the domain to another account.[77] All traffic to the domain name was redirected to a temporary site claiming the domain was for sale.[78] The temporary site listed an email address for information, and upon sending a domain transfer request, Solid Host sent a reply with a demand of $12,000. Solid Host claimed that defendant Namecheap, Inc. ("Namecheap") should be contributorily liable, as it provided the service "WhoisGuard," which listed Namecheap as the registrant, allowing the hijacker to remain anonymous.[79]

Namecheap had refused to reveal its customer's identity, even when provided with sworn affidavits by Solid Host's owner, reasoning they wanted to "remain neutral," and that the dispute was between Solid Host and the anonymous third party.[80]

The court made clear that this case is not a typical cybersquatting case—in which the cybersquatter registers the domain name of a well-known trademark as a speculation—but squatting by hacking.[81] Both types of cybersquatting, however, entail an effort by the squatter to ransom the domain name.[82]

---

[75] *Id.*
[76] 652 F. Supp. 2d 1092 (C.D. Cal. 2009).
[77] *Id.* at 1096–97
[78] *Id.* at 1097.
[79] *Id.* at 1096–97.
[80] *Id.* at 1098 (stating Namecheap eventually revealed the identity after receiving a court order directing them to cooperate with eNom to transfer the domain name to Solid Host).
[81] *Id.* at 1102.
[82] *Id.*

In determining contributory liability, the court looked to *Ford Motor Co.*[83] The three primary questions were (1) whether Namecheap sufficiently monitored and controlled the service; (2) whether Namecheap knew of the cybersquatting and; (3) whether the customer was doing so with bad faith intent to profit from the Solid Host mark.[84] As to the first requirement, the court answered affirmatively, reasoning that the anonymity service "was central to Doe's cybersquatting scheme," and "[i]f NameCheap had returned the domain name to Solid Host, Doe's illegal activity would have ceased."[85] As for the second requirement, the court stated that in Namecheap's inherently difficult position, as a registrar, Namecheap could not be expected to monitor the Internet to ascertain a customer's good or bad faith and, "that 'exceptional circumstances' must be shown to prove the degree of knowledge required to impose contributory liability for cybersquatting."[86] Because Solid Host's owners offered affidavits for the facts, the court did not accept Namecheap's motion to dismiss. Thus, the court recognized the applicability of a cause of action for contributory cybersquatting, as the information provided probably "would have led a normal and prudent person to conclude that the domain it registered had been stolen."[87]

C. Microsoft Corp. v. Shah[88]

Like in *Ford Motor Co.,* the defendants in *Microsoft Corp.* registered domains containing plaintiff's trademarks to divert traffic to their website.[89] However, unlike in *Ford Motor Co.* where inducement was not an issue, the defendants in *Microsoft Corp.* also actively provided instructions to customers on how to

[83] *Id.* at 1112, 1115; Ford Motor Co. v. Greatdomains.Com, 177 F. Supp. 2d 635, 646 (E.D. Mich. 2001).
[84] *Solid Host*, 652 F. Supp. 2d at 1115–16.
[85] *Id.*
[86] *Id.* (citing *Ford Motor Co*., 177 F. Supp. 2d at 647).
[87] *Id.* at 1116.
[88] C10-0653 RSM, 2011 WL 108954 (W.D. Wash. Jan. 12, 2011).
[89] *Id.* at *2.

mislead consumers to enter their sites and to use Microsoft logos without authorization.[90] Defendants also sold an emoticon-related software that incorporated Microsoft marks.[91] The defendants did not "simply provide a marketplace where a trade in domain names may take place, as was the case in" *Ford Motor Co*.[92] Rather, the defendants developed and marketed a method, of which "the sole purpose . . . was to allow purchasers to profit from the illicit use of Microsoft marks" by misleading web-surfers to think that they were browsing the sites of authorized Microsoft retailers.[93] Interestingly, the court in *Microsoft Corp.* relied on both the "flea market" model set forth in *Ford Motor Co.*, and *Solid Host,* in addition to traditional trademark principles for contributory trademark dilution as used in *Inwood*.[94]

In analyzing the ACPA, the court found Shah's conduct to fall "squarely within the statute's goal of imposing liability on those who seek to profit in bad faith by means of registering, trafficking, or using domain names that contain identical or confusingly similar marks."[95] The defendants' conduct of selling a method that teaches third parties about how to infringe on the core rights, against which the ACPA was enacted to protect, "should not be able to escape liability by interpreting the statute so narrowly."[96] Finally, the court relied on *Bob Jones Univ. v. United States*, which makes clear that "it is a well-established canon of statutory construction that a court should go beyond the literal language of a statute if reliance on that language would defeat the plain purpose of the statute."[97]

---

[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.* at *3.
[94] *Id.* at *2 (referencing a similar case, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996)).
[95] *Id.* at *3.
[96] *Id.*
[97] *Id.* at *3 (quoting Bob Jones Univ. v. United States, 461 U.S. 574, 586 (1983)).

The court found that the defendants could not hide behind the protection of blindness to the bad faith reasons behind the sales of the product.[98] Because *Microsoft Corp*. dealt with a markedly more aggressive behavior—developing and marketing a tool helping its customers to infringe on the Microsoft marks through its marketplace—the defendants' conduct satisfied the elevated bad faith standard from *Ford Motor Co.* as the "cyber-landlord" had reason to know that its "vendors [were] utilizing the marketplace for domain names" with no "legitimate purpose."[99]

In finding contributory infringement, the court took a more cautious road than previous courts and relied on the Ninth Circuit decision, *DSPT International v. Nahum*.[100] The defendant in *DSPT* used the plaintiff's mark to gain an advantage in bargaining for money that was arguably owed to him.[101] The court held that even though the ACPA was enacted to stop cybersquatters registering hundreds of domain names, the statute "is written more broadly than what may have been the political catalyst that got it passed."[102] Thus, the court interpreted the Act broadly to include such bad faith use.

D. Verizon California, Inc. v. Above.com[103]

Above.com, an ICANN accredited domain name registrar,[104] offered (and still offers) so-called WHOIS privacy services and

---

[98] *Id.*

[99] *Id.* at *2.

[100] *Id.* at *3 (citing DSPT International v. Nahum, No. 08–55062 2010 WL 4227883 *3 (9th Cir. Oct 27, 2010) (holding that defendant had used plaintiff's mark to gain leverage in bargaining for money that someone arguably owed to him)).

[101] *Id.* at *8.

[102] *Id.* (quoting *DSPT International*, No. 08–55062 at *3).

[103] Verizon Cal., Inc. v. Above.com Pty, Ltd., 881 F. Supp. 2d 1173 (C.D. Cal. 2011).

[104] *See How to Become a Registrar*, ICANN, https://www.icann.org/resources/pages/accreditation-2012-02-25-en (last visited April 15, 2015).

domain parking services.[105] Ten unknown "John Does" registered over a hundred domain name variants and typographically erroneous[106]—yet similar—domain names to Verizon and other famous-mark holders through Above.com.[107] Although it is clear that a registrar cannot be held liable for merely registering domain names, [108] the offering of WHOIS privacy and domain parking—both of which increased Above.com income per domain name—incentivized the registrants to register domain names with bad faith intent to profit to generate domain names similar to famous marks. The reason for this is that the parked sites display various related advertisements, which in turn pay a certain amount per click to the registrant. In short, the similar domain name lures unknowing consumers to the site, which generates traffic and subsequent clicks.

Because the court found that a registrar's registration of a domain name implicates a service, it relied on *Lockheed Martin Corp.*'s extent of control and monitoring of the instrumentality used by the Does to infringe on the marks.[109] It further agreed with *Ford Motor Co.* and *Solid Host* that bad faith intent to profit must be demonstrated by the existence of exceptional circumstances.[110] As direct liability had been properly alleged for the domain names

---

[105] *Verizon Cal., Inc.*, 881 F. Supp. 2d at 1175.

[106] This practice is also known as "Typo-squatting."

[107] *Verizon Cal., Inc.,* 881 F. Supp. 2d at n.2. The court found that "Defendants have registered ''www.ver9izon.com,'' ''www.veri9zon.com,''and ''www.verizo9n.com.'' On a standard computer keyboard, the ''9'' key straddles the ''i'' and ''o'' keys; thus, a consumer might mistakenly hit the ''9'' while typing in ''www.verizon.com'' and inadvertently visit one of Defendants' sites, rather than Verizon's." *Id.* at n.1.

[108] *See id.*

[109] *Id.* at 1180 (quoting Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999)).

[110] *Id.*; Ford Motor Co. v. Greatdomains.Com, 177 F. Supp. 2d 635, 647 (E.D. Mich. 2001); *see also* Solid Host v. Namecheap Inc., 652 F. Supp. 2d 1092, 1116 (C.D. Cal. 2009) (holding "'exceptional circumstances' must be shown to prove the degree of knowledge required to impose contributory liability for cybersquatting").

in question, the case turned on whether the facts presented "plausibly demonstrate the exceptional circumstances necessary to show that the defendants knew or should have known that the registrants were violating the ACPA in bad faith."[111] The defendants both controlled and monitored the privacy and parking services, and knew that the services were used to cybersquat on plaintiff's famous marks.[112] Furthermore, both services clearly incentivize registrants to cybersquat, who "should have been aware" that they could be used for cybersquatting.[113] Further, the service had already been subject to "nearly 200 UDRP cybersquatting complaints."[114]

In determining the availability of ACPA contributory cybersquatting liability, the court looked to all three previously mentioned cases, all of which either expressly confirmed the existence of such an action, or at least suggested that contributory liability may exist.[115] Unlike the previous cases, the court in *Verizon California* made an effort to mention the most fundamental step in any legal analysis, which is always to "look to

---

[111] *Verizon Cal., Inc.*, 881 F. Supp. 2d at 1180.

[112] *Id.*

[113] *Id.*

[114] *Id.*; *see* § 4 Uniform Domain Name Dispute Resolution Policy (1999), https://www.icann.org/resources/pages/policy-2012-02-25-en (UDRP is a mandatory administrative proceeding for all gTLD, and some ccTLD disputes for complaints regarding domain registrations that "(i) . . . is identical or confusingly similar to a trademark or service mark in which the complainant has rights;" and the registrant has (ii) "no rights or legitimate interests in respect of the domain," and (iii) the domain "has been registered and is being used in bad faith."); *see, e.g.*, WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP), http://www.wipo.int/amc/en/domains/guide/#a1 (UDRP proceedings are generally faster and more inexpensive than regular procedure).

[115] *See* Microsoft Corp. v. Shah, No. C10–0653 RSM, 2011 WL 108954, at *1–*3 (W.D. Wash. Jan. 12, 2011); Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1111–17 (C.D. Cal. 2009); Ford Motor Co. v. Greatdomains.com, Inc., 177 F. Supp. 2d 635, 646–47 (E.D. Mich. 2001).

the statute's text."[116] The court reiterated that the ACPA does not "expressly [recognize] nor expressly prohibit . . . claim[s] for contributory cybersquatting."[117] Contributory liability for trademark infringement already existed and continues to exist, and like under the ACPA, is a purely judicially created doctrine derived from the common law of torts.[118] As such, the court based its further discussion on the Supreme Court case *United States v. Texas*,[119] which held that it is presumed that when a statute "invade[s] the common law[, to] 'favor . . . the retention of long-established and familiar principles, except when a statutory purpose to the contrary is evident.'"[120] The court concluded that "[a]gainst this backdrop, Congress codified the ACPA as an extension of trademark law because the problems created by cybersquatting did not fit neatly into traditional trademark principles."[121]

The ACPA was introduced with the aim of combating cybersquatters operating outside the realm of commerce. The court concluded that Congress must have been aware of the contributory trademark infringement standards set in common law, and without an "expressed legislative desire to the contrary, the ACPA carried forward traditional common law principles attendant to trademark rights."[122] It did not matter, for the sake of applying contributory liability, that the ACPA (unlike the Lanham Act) requires proof of bad faith intent to profit.[123] Requiring such proof automatically

[116] *Verizon Cal., Inc.,* 881 F. Supp. 2d at 1176 (citing Hawaii v. Office of Hawaiian Affairs, 556 U.S. 163, 173–75 (2009)).

[117] *Id.*

[118] *Id.* at 1177 (quoting Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 104 (2d Cir. 2010)).

[119] *Id.* (quoting U.S. v. Texas, 507 U.S. 529, 534 (1993)).

[120] *Id.* at 1176–77 (quoting Isbrandtsen Co. v. Johnson, 343 U.S. 779, 783 (1952) and Astoria Federal Savings & Loan Ass'n. v. Solimino, 501 U.S. 104, 108, (1991)).

[121] *Id.*; *see also* S. REP. No. 106–140, at 4 (1999).

[122] *Verizon Cal., Inc.,* 881 F. Supp. 2d at 1177–78.

[123] *Id.* at 1178.

raises the bar for imposing liability.[124] This heightened standard fits squarely in the present scenario because for the registrar to be liable, it is not enough that it is aware of a similar domain name, it must also know that the domain is registered in bad faith.[125] This, in turn, presents a stricter rule than for contributory trademark infringement. Although the defendant pointed to legislative history which indicates that the ACPA was intended to be narrow, contributory liability is "sufficiently cabined by the 'exceptional circumstances' requirement to prevent the imposition of liability in contravention of the intent of the statute."[126]

In other words, according to the court, no innocent registrar, irrespective of offering WHOIS-masking and domain parking services, may be held liable for a registrant's bad faith domain name registration.[127]

IV. ANALYSIS OF PETROLIAM NASIONAL BERHAD V. GODADDY.COM, INC.

Petroliam Nasional Berhad v. GoDaddy.com, Inc. was presented to the Ninth Circuit appellate court by plaintiff-appellant Petroliam Nasional Berhad ("Petronas"), after the U.S. District Court for the Northern District of California granted summary judgment in favor of registrar GoDaddy.com, holding that the ACPA did not include a cause of action for contributory cybersquatting.[128] The Ninth Circuit affirmed.

One or more "John Does" had registered the domain names petronastower.net and petronastowers.net with a third party registrar in 2003.[129] The underlying issue evolved around the

---

[124] *Id.*
[125] *Id.* at 1179.
[126] *Id.*
[127] *Id.*
[128] Petroliam Nasional Berhad v. GoDaddy.com, Inc., 737 F.3d 856 (N.D. Cal. 2012), *aff'd*, 737 F.3d 546 (9th Cir. 2013), *cert. denied*, 13-1255, 2014 WL 1496428 (U.S. Oct. 6, 2014).
[129] *Id.* at 548.

Does' transferal of the domain names to GoDaddy.com in 2007 and subsequent utilization of the GoDaddy.com WHOIS anonymization service and domain parking service. This allowed the Does to point the domain names to a pornographic website hosted by a third party webhost.[130]

In determining whether the ACPA includes a cause of action for contributory cybersquatting, the court based its analysis on three main questions: (1) whether the plain text of the ACPA provides a cause of action and whether this was Congress' intent; (2) whether ACPA created a new and distinct cause of action; and (3) whether the goals of the ACPA would be advanced by allowing suits against registrars for contributory cybersquatting.[131]

A. *Is Contributory Cybersquatting Liability Authorized by the Plain Text of the ACPA?*

The court split the question of whether the text of the ACPA authorizes a cause of action for contributory cybersquatting into two subcategories, first looking at the text in isolation, and then analyzing Congress' intent in enacting 15 U.S.C. §§ 1125(d)(1)(A) and 1114(2)(D)(iii).

The court's first argument is that ACPA does not mention any forms of secondary liability and merely imposes civil liability for persons with "bad faith intent to profit" from a protected mark by "register[ing], traffic[king] in, or us[ing] a domain name."[132] It reasoned, by extending liability to registrars who are not themselves cybersquatters, one "would expand the range of conduct prohibited by the statute from a bad faith intent to cybersquat on a trademark to the mere maintenance of a domain name by a registrar, with or without a bad faith intent to profit."[133] The court draws its main argument from *Central Bank of Denver v. First Interstate Bank of Denver and Jack K. Naber*, in which the

[130] *Id.*
[131] *Id.* at 550.
[132] *Id.* (citing 15 U.S.C. § 1125(d)(1)(A)).
[133] *Id.* at 550–51.

Supreme Court did not accept plaintiff's assertion of an aiding and abetting claim under § 10(b) of the Securities Exchange Act.[134] They held, "[w]e cannot amend the statute to create liability for acts that are not themselves [prohibited] within the meaning of the statute."[135] because "when Congress enacts a statute under which a person may sue and recover damages from a private defendant for the defendant's violation of some statutory norm, there is no general presumption that the plaintiff may also sue aiders and abettors."[136]

Ultimately, the Ninth Circuit found that Congress' intent could not have been to include secondary liability by pointing to a portion of *Central Bank of Denver*, which implies that Congress knew of secondary liability and its uses in traditional trademark law, but actively chose not to add such a provision in the statute.[137]

Plaintiff-appellant also argued that the language in § 1114(2)(D)(iii) indicates that § 1125(d)(1)(A) was intended to "create a cause of action for secondary liability."[138] In analyzing this argument, the court looked at the statute and concluded the specific § 1114(2)(D)(iii) "applies only to 'this section,'" while § 1114 "sets out remedies for the entire Lanham Act."[139]

---

[134] Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164, 177–78 (1994) ("The issue, however, is not whether imposing private civil liability on aiders and abettors is good policy but whether aiding and abetting is covered by the statute;" . . . "The proscription does not include giving aid to a person who commits a manipulative or deceptive act."); 15 U.S.C. § 78j(b).

[135] *Cent. Bank*, 511 U.S. at 177–78.

[136] *Id.* at 182.

[137] *Petroliam*, 737 F.3d at 551; Pub. L. No. 106–113 (citing *Cent. Bank*, 511 U.S. at 178 ("Congress knew how to impose [secondary] liability when it chose to do so.")).

[138] *Petroliam*, 737 F.3d at 551.

[139] *Id.*; U.S.C. § 1114(2)(D)(iii) ("A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another *absent a showing of bad faith intent to profit* from such *registration* or *maintenance* of the domain name." (emphasis added)).

Finally, the court concluded that legislative history shows that § 1114(2)(D)(iii) was intended to "codify the protection granted [to] registrars in *Lockheed Martin Corp.*"[140] This was because *Lockheed Martin Corp.* "considered secondary liability of registrars for trademark infringement under 15 U.S.C. § 1125(a)."[141] The court could thus not find anything that suggested intent from Congress to include "a cause of action for contributory cybersquatting" in § 1125(d).[142]

B. *A New and Distinct Course of Action*

The Ninth Circuit did not agree with the previous district court cases, or plaintiff-appellant, that Congress incorporated "the common law of trademark, including contributory infringement, into the ACPA."[143] The court once again relied on *Central Bank of Denver* which stated that there is "no general presumption that the plaintiff may also sue aiders and abettors" when Congress enacts tort statutes relating to private defendants.[144] The court also disagreed with plaintiff-appellant's argument, presuming that there must be statutory purpose to the contrary of long-established and familiar principles before deviating from the common law.[145]

The court recognized that courts may infer a cause of action where "circumstances suggest that Congress intended to

---

[140] *Petroliam*, 737 F.3d at 551.

[141] *Id.* (citing S. REP. No. 106–140 at 11; *Lockheed Martin Corp*., 141 F. Supp. 2d at 655 ("The bill, as amended, also promotes the continued ease and efficiency users of the current registration system enjoy by codifying current case law limiting the secondary liability of domain name registrars and registries for the act of registration of a domain name.")).

[142] *Petroliam*, 737 F.3d at 551.

[143] *Id.*; Verizon California, Inc. 881 F. Supp. 2d 1173, 1176–79 (C.D. Cal. 2011); Microsoft Corp. v. Shah, No. 10–0653, 2011 WL 108954, at *1–*3 (W.D. Wash. Jan. 12, 2011); Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1111–12 (C.D. Cal. 2009); Ford Motor Co. v. Greatdomains.com, Inc., 177 F. Supp. 2d 635, 646–47 (E.D. Mich. 2001).

[144] *Petroliam*, 737 F.3d at 552 (citing Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164, 182 (1994)).

[145] *Id.*

incorporate common law principles into a statute."[146] However, the court was not able to find such "circumstances" in this case.[147] The differences between traditional Lanham Act claims and ACPA claims separate the ACPA from the accumulated common law that the Lanham Act is based upon.[148] This is because the court read the ACPA as a "new statutory cause of action" created "to address a new problem: cybersquatting."[149] The purpose of the statute was, in other words, distinct from traditional trademark law because traditional trademark law "only restricts commercial use of another's protected mark in order to avoid consumer confusion as to the source of a particular product."[150] Since the trademark owner must prove "bad faith" to find cybersquatting liability, "no analogous requirement exists for traditional trademark claims."[151] The court further draws analogy to actions established by the Digital Millennium Copyright Act ("DMCA"), which the Ninth Circuit found to not be necessarily subject to the "same defenses available to traditional copyright claims."[152]

C. *Furtherance of the Statute's Goals*

The court next looked at the legislative history, which states that the ACPA was enacted to "protect consumers . . . and to provide clarity in the law for trademark owners by prohibiting the bad-faith and abusive registration of distinctive marks."[153] The court's interpretation of the Senate report was that the ACPA was "carefully and narrowly tailored" with the purpose to fix the

---

[146] *Id.*
[147] *Id.*
[148] *Id*. at 553.
[149] *Id.* at 552 (citing S. REP. No. 106-140, at 7) (noting that "[c]urrent law does not expressly prohibit the act of cybersquatting").
[150] *Id.*; *see generally* New Kids on the Block v. News Am. Pub., Inc., 971 F.2d 302, 305–06 (9th Cir. 1992); Bosley, 403 F.3d 672, 680 (9th Cir. 2005).
[151] *Petroliam*, 737 F.3d at 552–53.
[152] *Id.*; MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 948 n.10 (9th Cir. 2011).
[153] *Petroliam*, 737 F.3d at 553 (citing S. REP. No. 106–140, at 4).

specific problem of cybersquatting.[154] This view is strengthened by looking at the actual limitations included in the Act, namely the requirement for bad faith,[155] and the narrow definition of who "uses" a domain name.[156] By broadening the Act to impose secondary liability, the scope of the Act would expand to a level that would "seriously undermine both these limiting provisions."[157]

The previous district court cases remedied this issue by requiring a plaintiff to show "exceptional circumstances."[158] The Ninth Circuit did not accept this solution, as it has "no basis in either the Act, or in the common law of trademark. Rather than attempt to cabin a judicially discovered cause of action for contributory cybersquatting with a limitation created out of whole cloth, we simply decline to recognize such a cause of action in the first place."[159] The last argument the court presented was the consideration of efficiency, specifically that the ACPA cybersquatting provision requires subjective bad faith, and the application of direct liability "spares neutral third party service providers from having to divine the intent of their customers."[160] It

---

[154] S. REP. No. 106–140, at 12–13.

[155] *Petroliam*, 737 F.3d at 546, 553; 15 U.S.C. § 1125(d)(1)(A)(i) (2012) ("*A person* shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section[.]" (emphasis added)).

[156] *Id.*; 15 U.S.C. § 1125(d)(1)(B) (2012) ("In determining whether a *person* has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to--"); § 1125(d)(1)(D) ("A *person* shall be liable for using a domain name under subparagraph (A) *only if that person is the domain name registrant* or that registrant's *authorized licensee*.") (emphasis added).

[157] *Petroliam*, 737 F.3d at 553.

[158] *Id.*; Verizon California, Inc. v. Above.com Pty Ltd., 881 F.Supp.2d 1173, 1180 (C.D. Cal. 2011); Microsoft Corp v. Shah, No. C10-0653 RSM, 2011 WL 108954, at *2 (W.D. Wash. Jan. 12, 2011); Ford Motor Co. v. Greatdomains.com, Inc., 177 F.Supp.2d 635, 647 (E.D. Mich. 2001).

[159] *Petroliam*, 737 F.3d at 553.

[160] *Id.*

is thus more efficient to analyze a registrant's subjective intent in relation to each domain, rather than having big corporations such as GoDaddy.com having to screen each registration.[161]

The court regarded the ACPA's explicitly listed remedies (excluding contributory liability) as sufficient for the purposes of fighting cybersquatting.[162] This is strengthened by the *in rem* provision, which under certain conditions allows the trademark holder to sue the domain instead of the registrant *in personam*.[163] Trademark holders may also bring traditional or secondary trademark infringement claims that arise from cybersquatting activities.[164]

V. IS THE *PETROLIAM* DECISION CORRECT?

The Ninth Circuit did indeed take the safe route by remaining well within the literal text of the ACPA, leaving the future of contributory cybersquatting liability in the hands of Congress or the Supreme Court.

Interestingly, the district courts in *Ford Motor Co., Solid Host, Microsoft Corp.*, and *Verizon California* dared to do much more. One can easily reason that Congress would—and should have—included a secondary liability provision within the ACPA if that was its intent. This argument, however, is not immediately persuasive, because as the Ninth Circuit stated, the ACPA was enacted to address a specific problem that the current Lanham Act was unable to deal with. The issue of cybersquatting obviously did not exist before the enactment of the Lanham Act; in fact, it was not an issue until the 1990's when the modern DNS caught on with the general public. Intellectual property laws are made to protect an industry segment that is constantly evolving. New technology often outrun statutory definitions. This is abused by infringers.

---

[161] *Id.* (referencing that GoDaddy.com's registrants holds over 50 million domains).

[162] *Id.*

[163] *Id.*; 15 U.S.C. § 1125(d)(2)(A) (2012).

[164] *Petroliam*, 737 F.3d at 553.

Every tool available should be used to find an equitable solution. If relevant common law exists, it should not simply be discarded, but interpreted with the statute, in light of the dynamic technical landscape. The ACPA is a tool for trademark owners to stop cybersquatting; it gives courts the necessary authority to cancel or transfer the domain names to the trademark owners in situations where the registrant is not acting in commerce. The courts cannot allow themselves to look away from the massive trademark common law just because of this technicality. The fact that the *in rem* provision and the UDRP procedures are very effective in combating direct cybersquatting is not reason enough to deny the application of secondary liability where the contributor has had an active role in the primary cybersquatting activity.

A. *The Plain Text of ACPA*

The ACPA, like the Lanham Act for traditional trademarks, does not contain any explicit text for contributory liability. With regard to 15 U.S.C. § 1125(d)(1)(A), the *Petroliam* appellate court emphasized that by holding registrars accountable, the "range of conduct prohibited by the statute from a bad faith intent to cybersquat on a trademark *to the mere maintenance of a domain name by a registrar, with or without bad faith intent to profit*" would be too substantial an expansion of the statute.[165] This interpretation is too restrictive. If anything, the district court's interpretation follows a strict standard in which registrars, who are not acting in bad faith, cannot be held liable. Another issue with the Ninth Circuit's justification is that its primary source is *Central Bank of Denver*, in which the Supreme Court stated that "Congress knew how to impose [secondary] liability when it chose to do so."[166] *Central Bank of Denver* involves a different issue: the general antifraud provision in the Securities Exchange Act ("SEA") § 10(b). This provision presents substantially different

[165] *Id.* at 150 (emphasis added).
[166] Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 114 S.Ct. 1439, 1148 (1994).

considerations than trademark law.[167] Trademark law, unlike securities law, is designed to protect owners' trademarks from being misrepresented to the relevant consumer base.

In examining the enactment of the Lanham Act back in 1946, why did the courts not end up with a similar result as in *Central Bank of Denver* when discussing the application of traditional contributory trademark infringement? The *Inwood* court did find contributory trademark infringement, even though the Lanham Act did not expressly justify its application. The short answer is that substantial common law supported such application. Substantial common law background was not an issue in *Central Bank of Denver*. To that, the Ninth Circuit argues contributory cybersquatting liability involves a new and distinct course of action.[168]

As for the Ninth Circuit's discussion regarding § 1114(2)(D)(iii), the Ninth Circuit's justification is principally correct. The provision clearly states "under this section," but that only excludes § 1114(2)(D)(iii) specific applicability, as the Ninth Circuit infers that this is an argument against applying secondary liability in cybersquatting cases, the provision just as much proves the opposite. Neither § 1114(2)(D)(iii) or any other provision in the Lanham Act expressly denies the applicability of contributory liability. It is unclear why the section should be treated in isolation from the rest of the section. The provision is not in a vacuum; it indirectly shows Congress' intent and consideration of applying secondary liability in certain scenarios.

It makes sense to apply the provision analogically to situations that are not mentioned in the provision. For example, it should apply to situations where the registrars' primary functions go beyond registration or maintenance of domain names. The registrars' safe harbor is intended for actions made as a registrar and not for profit-generating side businesses such as

---

[167] 15 U.S.C. § 78(j) (2012).
[168] *See infra* Part V.B.

WHOIS-masking and domain parking services. Furthermore, the provision clearly states that the registrars indeed are liable for registration and maintenance of domain names if found to have had "bad faith intent." This shows Congress' clear intent of holding dishonest registrars liable.

B. *New and Distinct Course of Action*

The appellant-defendant relied on *Inwood* and the application of contributory liability for trademark infringement under the Lanham Act.[169] The fact that Congress legislated against this legal background and placed the ACPA within the Lanham Act, shows that the intention must have been to include a cause of action for contributory cybersquatting.[170] The appellate court, admitted that even by relying on *Bank of Denver*, which infers that there "is no general presumption that the plaintiff may also sue aiders and abettors," "courts can infer such a cause of action where circumstances suggest that Congress intended to incorporate common law principles into [the Lanham Act]."[171] The Ninth Circuit however, would not find circumstances regarding the enactment of the ACPA that supports an argument of Congress' intent of incorporating theories of secondary liability into that Act.[172] This is because the Ninth Circuit claimed "the ACPA did not result from the codification of common law, much less common law that included a cause of action for secondary liability"; rather the ACPA was created to deal with a new, specific problem, cybersquatting, and thus created a new statutory cause of

[169] *Petroliam*, 737 F.3d at 553.

[170] *Id.* (citing United States v. Texas, 507 U.S. 529, 534 (1993)) ("Statutes which invade the common law . . . are to be read with a presumption favoring the retention of long-established and familiar principles, except when a statutory purpose to the contrary is evident.") (citations omitted).

[171] *Bank of Denver*, 114 S.Ct. at 1451; Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, n.2 (1982).

[172] *Bank of Denver*, 114 S.Ct. at 1452.

action.[173] The Ninth Circuit supports its decision and relies on both the substantial history behind the Lanham Act, originating from English common law,[174] and the law review article *The Illegitimacy of Trademark Incontestability,* which states that "the Lanham Act's primary, express purpose was to codify the existing common law of trademarks and not to create any new trademark rights."[175]

The Court claims that the ACPA has distinct purposes that differ from traditional trademark law, and thus must have distinct elements.[176] The main argument is that traditional trademark law prohibits commercial acts that infringe on another's mark in order to avoid source-identifying consumer confusion.[177] For finding cybersquatting liability, there is no requirement that the acts be "in commerce," but rather there must be "bad faith intent to profit."[178] Since traditional trademark law has no analogous requirement, the Ninth Circuit concludes that "bad faith intent to profit" is to be considered a distinct course of action.[179]

It is hard to argue against the fact that the ACPA is a new action *per se*. It is an action created to deal with a new type of infringement, cybersquatting, which did not exist at the enactment of the Lanham Act. However, common law is not static. Many cybersquatters do not act "in commerce" as there is no requirement for registrants to act in commerce to register domains (unlike for

[173] *Petroliam*, 737 F.3d at 552 (citing S. REP. No. 106–140, at 7 ("noting that '[c]urrent law does not expressly prohibit the act of cybersquatting'")).

[174] *Id.; see also* Moseley v. V Secret Catalogue, Inc., 123 S.Ct. 1115, 1122 (2003).

[175] *Petroliam*, 737 F.3d at 552 (citing Kenneth L. Port, *The Illegitimacy of Trademark Incontestability*, 26 IND. L. REV. 519, 520 (1993)).

[176] *Petroliam*, 737 F.3d at 552.

[177] *Id.*; *see also* New Kids on the Block v. News Am. Pub., Inc., 971 F.2d 302, 305–06 (9th Cir.1992); Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 680 (9th Cir. 2005).

[178] *Petroliam*, 737 F.3d at 552; 15 U.S.C. § 1125(d)(1)(B) (2012) (stating a person is "liable in a civil action by the owner of a mark" if that person has a "bad faith intent to profit from that mark").

[179] *Petroliam*, 717 F.3d at 553.

registering trademarks). It is also much cheaper and easier to register multiple domain names, unlike trademarks.[180] For example, a person, not acting in commerce, who registers a dot-com domain of a famous mark, and subsequently points the domain to explicit and obscene pornographic materials would be regarded as tarnishing and/or diluting the mark. Why should liability not be imposed on him, when his friend who acts in commerce (such as selling such merchandise across state borders) could be held liable?

The fact that the ACPA implements liability on "bad faith" instead of "in commerce" does not necessarily create a new cause of action. It rests on the same fundamental foundations, to protect the consumer from confusion as to the source of goods or services. "Bad faith" in the cybersquatting context infers a will to profit from the domain, similarly to someone "acting in commerce." The addition of the ACPA is merely a tool for the courts to be able to incur liability of cybersquatters without running afoul with the general wording of the Lanham Act, which was enacted almost seventy years ago.

C. *Furtherance of the Statute's Goals*

The Ninth Circuit claims that the legislative history and the Act in itself entail a narrow interpretation that precludes cybersquatting secondary liability. By looking at the Act in isolation, the analysis above shows that it warrants an expansive and analogic interpretation.[181] In analyzing the Senate Report, it is also difficult to support the Ninth Circuit's argument. The Report states that:

> The bill is carefully and narrowly tailored, however, to extend only to cases where the plaintiff can demonstrate that the defendant registered, trafficked in, or used the offending domain name with bad-faith intent to profit from the goodwill of a mark belonging to someone else. Thus,

---

[180] An interesting side note could be made towards regulation of the .no (Norwegian country code TLD), which until June 1, 2014 required every registrant to provide an organization number in order to register domain names. A direct result of this was that all registrants acted in commerce.

[181] *See supra* Part V.A.

> the bill does not extent [sic] to innocent domain name registrations by those who are unaware of another's use of the name, or even to someone who is aware o the trademark status of the name but registers a domain name containing the mark for any reason other than with bad faith intent to profit from the goodwill associated with that mark.[182]

Congress' aim with this is to limit the application to the registrant's bad faith registration. It is "carefully and narrowly" tailored in the sense that registrants who are not registering the domain name in bad faith should not be liable. It does not address excluding secondary liability as the Ninth Circuit claims. The goal of the statute is to provide the courts an effective tool against cybersquatters (people not acting in commerce), who act with bad faith intent to profit on other's marks. The Act is "carefully and narrowly" tailored to not *catch* people registering domain names in good faith. *That is it.*

It is counterintuitive to presume that registrars knowingly contributing to primary cybersquatting activity get *carte blanche* to do so, by the mere fact that Congress has stated people registering domain names in good faith are outside of the ACPA's scope.

In an effort to harmonize the ACPA with traditional trademark infringement rules, the district courts in *Verizon California*, *Microsoft Corp.*, and *Ford Motor Co.* required a showing of "exceptional circumstances."[183] The Ninth Circuit claims the exceptional circumstance test "has no basis in either the Act, or in the common law of trademark."[184] Both the ACPA and Lanham Act are mute about contributory liability, so it is not sensible for Congress to have included the words "exceptional circumstances." It is also strange that the Court would mention the common law of trademark, as it already concluded the ACPA is a new and distinct course of action, rending the common law of trademarks irrelevant.

---

[182] S. REP. No. 106-140, at 12–13.

[183] *See* Verizon California, Inc. v. Above.com Pty Ltd., 881 F. Supp. 2d 1173, 1178 (C.D. Cal. 2011); Microsoft Corp v. Shah, No. C10-0653 RSM, 2011 WL 108954, at *2 (W.D. Wash. Jan. 12, 2011) ; Ford Motor Co. v. Greatdomains.com, Inc., 177 F. Supp.2d 635, 647 (E.D. Mich. 2001).

[184] *Petroliam*, 737 F.3d at 553.

The separation of powers dictates that it is up to Congress to enact laws. A federal court may not lightly create common law rights; it must exercise its authority to fill interstitial gaps to effectuate the statutory pattern enacted by Congress.[185] The *Ford Motor Co.* and *Solid Host* "exceptional circumstance" test is a way to fill an interstitial gap. It was clear that Namecheap sufficiently monitored and controlled its services, but for the court not to exceed its powers and overstep Congress' intent Namecheap would have to positively know that the domain had been stolen before placing contributory liability. This fits well into the realm of traditional trademark infringement and the Lanham Act because it aligns analogically with *Inwood* and the 20-plus years of decisions finding contributory trademark infringement without intervention by Congress. Namecheap continued to supply the anonymity service, even though it knew it was being used to cybersquat. The considerations are inherently similar.

The Ninth Circuit asserts, "[l]imiting claims under the Act to direct liability is also consistent with the ACPA's goal of ensuring that trademark holders can acquire and use domain names without having to pay ransom money to cybersquatters."[186] The last part of the statement is sensible. The ACPA's main purpose and weight rests on the ability for mark owners to get squatted domain names returned or cancelled. However, this does not exclude the assertion of secondary liability of registrars acting outside of the core registrar services (such as registering and maintaining domain

[185] *See* Hooven v. Exxon Mobil Corp., 465 F.3d 566, 573 n.5 (3rd Cir. 2006); *see also* Donald L. Doernberg, *Juridical Chameleons in the "New Erie" Canal*, 1990 UTAH L. REV. 759, 761 (1990) ("The Article concludes with the suggestion that federal courts have considerable common law powers, which, rather than being inconsistent with separation of powers, actually function to make exercises of congressional power more effective. Separation of powers is not offended when federal courts create common law, provided that these efforts are constrained by expressions of policy in positive law, the Constitution and federal statutes.").

[186] *Petroliam*, 737 F.3d at 553.

names)[187] and that are aware of and contribute to cybersquatting activity. The interests of registrars should not preempt a mark owner's right to pursue contributory infringing activity.

This Article does not demand that registrars "have to divine the intent of their customers," but rather to be attentive when receiving notification of cybersquatting activity by mark owners.[188] Although different in many key aspects, primarily by the fact the Act clearly authorize its applicability, one may look to the DMCA limitations on liability relating to material online, which indemnifies service providers for hosting infringing materials when promptly removing the infringing material upon discovery or notification.[189] The Ninth Circuit's fears of imposing registrars to "trademark and domain name disputes" is simply not realistic by the heightened standard set by the "exceptional circumstance" test.[190]

VI. CONCLUSION AND REFLECTIONS

The Ninth Circuit's reasoning is intriguing, and on many levels persuasive. It remains well within the literal letter of the statute, leaving the matter for the Supreme Court or Congress to decide. The Ninth Circuit has done its job well within its discretion, so why argue against its holding?

The Supreme Court in *Brown v. Duchesne,* in 1856, stated "it is well settled that, in interpreting a statute, the court will not look merely to a particular clause in which general words may be used, but will take in connection with it the whole statute . . . and the objects and policy of the law."[191] This principle was further elaborated in *Bob Jones* which made it clear that "[i]t is a well-established canon of statutory construction that a court should go beyond the literal language of a statute if reliance on that

[187] *See also* 15 U.S.C. § 1114(D)(iii) (2012) (safe harbor provision).
[188] *Id.*
[189] 17 U.S.C. § 512(g) (2012).
[190] *Petroliam,* 737 F.3d at 553.
[191] Brown v. Duchesne, 60 U.S. 183, 194 (1856).

language would defeat the plain purpose of the statute."[192] Both the objectives and policy considerations behind the ACPA and the Lanham Act conform to an expanded interpretation in support of contributory cybersquatting liability.

Although the Ninth Circuit abstained from discussing the "exceptional circumstance" test in *Petroliam*, the registrar acted less culpably than in *Solid Host* and *Microsoft Corp.,* this suggests that any reasonable court, by applying the "exceptional circumstance" test, might have found GoDaddy.com not liable for contributory cybersquatting. The Court's wording in *Petroliam* effectively removed any hope for mark owner to get remedy against registrars contributing to cybersquatting in the Ninth Circuit. As discussed in Part V, this is unreasonably strict, considering the reason for imposing such secondary liability.

It is easy to imagine situations where a registrar should be held accountable for contributing to cybersquatting. The harm done to a famous trademark, such as by directing unknowing consumers to pornographic and other obscene websites, can be massive. This loss, in many cases, cannot be recovered from the primary cybersquatter as either *in personam* jurisdiction is unobtainable, or the defendant simply lacks the funds to cover profits, damages and legal costs,[193] or the maximum of $100,000 of statutory damages.[194]

The threshold for imposing liability should be high, but present, so as to function as a motivator for registrars to avoid actively contributing to cybersquatting. Registrars conducting their regular core businesses, such as registering domain names and maintaining their records should never lead to liability.[195] For a registrar to risk secondary cybersquatting liability a plaintiff should have to prove that: (1) someone registered a domain name with "bad faith intent to profit;" (2) the domain name registrar is acting

[192] Bob Jones Univ. v. United States, 461 U.S. 574, 586 (1983).
[193] 15 U.S.C. § 1117(a) (2012).
[194] *Id.* § 1117(d).
[195] *See id.* § 1114(D)(iii) (2012).

outside of its core functions of registering and maintaining domain names, as by offering services such as WHOIS-masking or domain forwarding; and (3) the existence of "exceptional circumstances." Such circumstances might be the registrar actively inducing the cybersquatting activity, such as by marketing services that helps the cybersquatters more efficiently squat on domains and trademarks alike, as seen in *Microsoft Corp*.[196] It might also entail more passive contribution or facilitation, such as hiding the cybersquatter's identity by publishing the cybersquatter's own information in the WHOIS record rather than the registrant's. There should be no passive contribution, unless the situation of offering such services would have led a normal and prudent person to conclude that the domain in question was squatted. This Essay does not contend that services going outside the scope of registering and maintaining domain names should automatically be viewed as bad faith or unlawful. Both WHOIS-masking and domain forwarding are practical tools that primarily serve legitimate purposes. As such, a registrar should only be liable when sufficiently notified by a mark owner of specific illicit use.

The Ninth Circuit rests its holding on efficiency considerations, namely that the ACPA cybersquatting provision requires subjective bad faith, and the application of direct liability "spares neutral third party service providers from having to divine the intent of their customers."[197] The Court uses the words "neutral third party," but how can the cases as analyzed above, and the above several hypotheticals signify a "neutral third party"? Admittedly, the registrars act in varying levels of involvement and guilt, but it must be underlined that registrars very well may behave directly culpably and should be held contributorially liable.

Major registrars such as GoDaddy.com have already implemented steps to counter the likelihood of secondary cybersquatting liability when offering services such as

[196] *See* Microsoft Corp v. Shah, No. C10-0653 RSM, 2011 WL 108954, at *2 (W.D. Wash. Jan. 12, 2011).

[197] *Petroliam,* 737 F.3d at 553.

WHOIS-masking and sponsored domain-parking services by including various provisions in their service agreements. The GoDaddy.com's Domain Name Proxy Agreement authorizes GoDaddy.com to disclose personal information to "[r]esolve any and all third party claims, whether threatened or made, arising out of [the registrants] use of a domain name for which [GoDaddy.com subsidiary company, Domains By Proxy, LLC] is the registrant listed in the "Whois" directory on [the registrant's] behalf."[198] As for sponsored domain parking, which GoDaddy.com calls "Cashparking," GoDaddy.com clearly states in its Service Agreement that they "reserve the right to screen domain names prior to enrollment and . . . may exclude, in [its] sole discretion, any domain name for any reason, including, but not limited to: a) violation of this Agreement or the Universal Terms of Service; or b) infringement, or potential infringement, of a *third party* intellectual property right."[199] GoDaddy.com, in its various service agreements, refers to their general trademark policies that list an email address to contact to claim a trademark violation and GoDaddy.com's subsequent investigation procedures. This shows a great willingness to take trademark infringement and cybersquatting seriously and to find progressive solutions when available, without the mark owner having to initiate UDRP or ACPA proceedings against the direct cybersquatter or the domain *in rem.* This depicts a substantially different image than the Ninth Circuit portrays in *Petronas*.

GoDaddy.com's license agreements are a progressive example of how registrars can avoid secondary cybersquatting liability altogether. It shows how little effort it takes. As mentioned above,

---

[198] *See Domain Name Proxy Agreement Section 4.ii*, GODADDY http://www.godaddy.com/agreements/showdoc.aspx?pageid=DOMAIN_NAME PROXY (last visited Aug. 29, 2015).

[199] *See CASHPARKING® SERVICE AGREEMENT Section 2* GODADDY https://in.godaddy.com/agreements/ShowDoc.aspx?se=%2B&pageid=Cash_Park_SA (last visited Aug. 29, 2015) (emphasis added) (Cashparking is basically a default site provided by GoDaddy.com when registering domain names that contains advertisements whereas the registrant is paid based on traffic).

the inherent justification behind trademark law is the protection of consumers. By helping or inducing cybersquatters to make money by sponsored domain parking services, it is ultimately the consumer who loses both time and money trying to navigate to the correct website. Another loser is the mark owners, who have to police their marks and spend considerable amount of money towards UDRP proceedings and federal court proceedings. The additional cost imposed by the registrars' services such as domain masking and sponsored domain parking ultimately shifts to the consumer, as the product cost is increased as a measure to offset the policing cost.

It is only fair that some of this cost is transferred to the registrars who choose to go outside of the core services such as registering and maintaining domain names.