

Winter 2017

Contributory Liability Under the ACPA: A More Effective Approach to Deterring Cybersquatting at Its Source

Andrew J. Piombino

Follow this and additional works at: http://docs.rwu.edu/rwu_LR

 Part of the [Intellectual Property Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Piombino, Andrew J. (2017) "Contributory Liability Under the ACPA: A More Effective Approach to Deterring Cybersquatting at Its Source," *Roger Williams University Law Review*: Vol. 22 : Iss. 1 , Article 9.
Available at: http://docs.rwu.edu/rwu_LR/vol22/iss1/9

This Article is brought to you for free and open access by the School of Law at DOCS@RWU. It has been accepted for inclusion in Roger Williams University Law Review by an authorized editor of DOCS@RWU. For more information, please contact mwu@rwu.edu.

Contributory Liability Under the ACPA: A More Effective Approach to Deterring Cybersquatting at Its Source

Andrew J. Piombino

INTRODUCTION

The issue of contributory cybersquatting arises from the enactment of the Anti-Cybersquatting Consumer Protection Act (ACPA) in 1999, which created a cause of action for registering, trafficking in, or using an internet domain name confusingly similar to, or dilutive of, a trademark or personal name.¹ The statute was enacted primarily to combat those who register domain names with the intent to hold them, and later sell them, at a premium to those who would actually make use of the domain name.² The statute permits a trademark owner to bring an action against a person who, with a bad faith intent to profit from a mark, registers, traffics in, or uses a domain name that is confusingly similar to the protected mark.³ The statute also lays out several factors for determining whether there is bad faith, and creates an *in rem* civil action against the domain name.⁴ Since its inception, the statute has been used as a tool to take action against those who make a business out of ransoming domain names by buying them, running skeleton websites and demanding large buyout costs from those who own trademarks in the subject

-
1. 15 U.S.C.A. § 1125(d) (Westlaw through Pub. L. No. 114-254).
 2. S. REP. NO. 106-140, at 4 (1999).
 3. 15 U.S.C.A. § 1125(d) (Westlaw).
 4. *Id.*

of the domain name and seek to run a legitimate website.⁵ It has only in a few instances, however, been used to demand relief from those large domain registrars that passively support cybersquatting activity.⁶

Since the creation of the statute, several plaintiffs have attempted to extend the reach of the statute by suing domain registrars and hosting services for catering to cybersquatters.⁷ Several district courts have weighed in on the issue with varying results, but only one case has made it to a United States appeals court.⁸ That case, *Petroliam Nasional Berhad v. GoDaddy.com, Inc.*, was a Ninth Circuit case that came down in December 2013.⁹ There, a Malaysian petroleum company, known colloquially as “Petronas,” sued GoDaddy for registering and providing forwarding services to a cybersquatter using the name www.petronastowers.com, even after Petronas requested that GoDaddy take down the domain name.¹⁰ The Ninth Circuit declined to create and apply an action for contributory cybersquatting against GoDaddy, offering several rationales:

- (1) the text of the Act does not apply to the conduct that would be actionable under such a theory; (2) Congress did not intend to implicitly include common law doctrines applicable to trademark infringement because the ACPA created a new cause of action that is distinct from traditional trademark remedies; and (3) allowing suits against registrars for contributory cybersquatting would not advance the goals of the statute.¹¹

5. 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, 535 (2012).

6. *See, e.g., Acad. of Motion Pictures Arts & Scis. v. GoDaddy.com, Inc.*, No. CV 10-03738, 2015 U.S. Dist. LEXIS 120871, at *66-67 (C.D. Cal. Sept. 10, 2015) (discussing whether GoDaddy acted with the requisite bad faith intent to find the company liable under the Anti-Cybersquatting Consumer Protection Act); *Verizon Cal., Inc. v. Above.com Pty, Ltd.*, 881 F. Supp. 2d 1173, 1179 (C.D. Cal. 2011) (concluding that contributory liability exists under the ACPA).

7. *See, e.g., Acad. of Motion Pictures Arts & Scis.*, 2015 U.S. Dist. LEXIS 120871, at *66-67; *Verizon Cal., Inc.*, 881 F. Supp. 2d at 1179.

8. *See Petroliam Nasional Berhad, (Petronas) v. GoDaddy.com, Inc.*, 737 F.3d 546 (9th Cir. 2013).

9. *Id.* at 546.

10. *Id.* at 548.

11. *Id.* at 550.

Implicit in this reasoning was a concern that registrars might be overburdened and more restricted in issuing new domain names if they had to divine the intent of those seeking to register domain names.¹² Further, the court, and many supporters of registrars think that the mechanisms in place for *in rem* suits and arbitration under the Uniform Domain Name Dispute Resolution Policy (UDRP) are more than sufficient to combat the problem.¹³ The United States Supreme Court denied certiorari in October 2014, likely due in large part to the lack of a circuit split, as only one appeals court had ruled on the issue.¹⁴

This note will argue that *Petronas* was decided incorrectly, and that the intent, language, and policy behind the ACPA implicitly creates an action for contributory cybersquatting against domain name registrars and hosting services that is necessary to protect the rights of trademark owners and beneficial for the streamlining of domain name disputes. Part I will provide an overview of the pervasive problem of cybersquatting, the response of Congress enacting the ACPA, and ACPA's effects on cybersquatting activities. It will address the statute's failure to speedily and properly protect trademark owners from cybersquatting as it is currently interpreted. Additionally, it will illustrate how those failures play out in the context of the *Petronas* case. Part II will argue that the history and nature of the ACPA implicitly creates an action for contributory cybersquatting by illustrating the history behind the act, comparing the addition of the ACPA to codification of trademark infringement as a whole, which allows for contributory liability under common law principles. Part III will argue that the goals of the ACPA support an action for contributory liability based on the statutory construction, the legislative history, and the goals driving the act. It will refute the policy arguments concerning an overly burdensome system for domain name registrars if they are required to divine the intent of potential domain owners, and the concern for rejection of domain registration for those who may not be acting in bad faith. Lastly, it will argue that the interests of trademark owners are not adequately protected by *in rem* provisions where damages are necessary to make them whole, and

12. *See id.* at 553.

13. *Id.* at 554.

14. *Id.* at 546, *cert. denied*, 135 S. Ct. 55 (2014).

that creating the action will incentivize domain name registrars to eliminate cybersquatters without the need for litigation. Finally, Part IV will conclude that the Supreme Court should take up this issue, and allow for an action for contributory cybersquatting for the protection of trademark owners and for purposes of expediency in resolving cybersquatting issues. It will propose that the Supreme Court might limit contributory liability by creating a more robust interpretation of the bad faith standard.

I. THE ELUSIVE PROBLEMS OF CYBERSQUATTING

Cybersquatting is a term that encompasses a series of practices plaguing trademark owners in the internet age, and that continues to threaten to hijack and undermine the goodwill of trademark owners, and in some cases even to extort them.¹⁵ The most common, and perhaps the earliest form, is the traditional cybersquatter, a person who registers a domain name including a well-known trademark for the purpose of selling the name to the trademark owner, often at an exorbitant price.¹⁶ Other practices that are subsumed under the title of cybersquatting include “typosquatting,” whereby a person registers misspellings of a trademark as a domain name in order to direct those who misspell a domain name to a different website, and “cyberpirating,” where a person uses the goodwill of the trademark to lure web users to a site, either by having it redirect to a different site, or merely connecting ad revenue from visitors to a fake one.¹⁷ Given the range of damage these different types of cybersquatting can cause based on their unique functions, the threat to a trademark holder is often far greater than the loss of money from being forced to buyout a cybersquatter, and can include tarnishment of the trademark and lost business opportunities.¹⁸

At the time of the enactment of the ACPA on November 29, 1999, it was clear that the mechanisms by which courts had dealt with cybersquatting activity up to that point were not sufficient,

15. See Robert L. Mitchell, *How Cybersquatters Tarnish Brand Names*, PC WORLD (Sept. 8, 2009, 1:47 PM), http://www.pcworld.com/article/171601/how_cybersquatters_tarnish_brand_names.html.

16. See *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1233 (N.D. Ill. 1996).

17. Tenesa S. Scaturro, *The Anticybersquatting Consumer Protection Act and the Uniform Domain Name Dispute Resolution Policy the First Decade: Looking Back and Adapting Forward*, 11 NEV. L.J. 877, 880 (2011).

18. *Id.* at 885; see also Mitchell, *supra* note 15.

since cybersquatters had become increasingly sophisticated in navigating loopholes in trademark infringement and dilution statutes, and because remedies under those statutes were uncertain and often very expensive to prosecute.¹⁹ The ACPA was created as a response, with the intention that it would close those loopholes by creating a more narrowly tailored statute which protects trademark owners from many types of cybersquatting uses by removing the “commercial use” requirement under the Federal Trademark Dilution Act (FDTA), while also creating a counterbalance by requiring bad faith in the alleged cybersquatter.²⁰ While the statute effectively addressed many of the concerns of the legislature at the time, it has been decidedly lacking in its ability to address the complicity of domain name registrars, who profit from registrations, and often hold the keys to speedy relief for trademark holders.²¹ Domain name registrars are organizations that have been accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) or a national country code top-level domain (TLD) (such as .uk or .ca) to register domain names.²² These companies sell domain names to the public, and act as a liaison between the consumer and domain registries such as VeriSign, which manages the

19. Scaturro, *supra* note 17, at 883.

20. 15 U.S.C. § 1125(d) provides, in relevant part:

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

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

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

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

(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 or section 220506 of Title 36.

15 U.S.C.A. § 1125(d) (Westlaw).

21. *See id.*

22. GODADDY, <https://www.godaddy.com/help/what-is-the-difference-between-a-registry-registrar-and-registrant-8039> (last visited Aug. 31, 2016).

registration of .com domain names.²³ Often, registrars such as GoDaddy.com also offer hosting and forwarding services, whereby they can provide servers to host a registrant's website, or cause the domain name to forward web users to a different domain name that the registrant owns.²⁴ Registrars, by their many functions, exercise a great deal of power over the registration and maintenance of domains. For that reason, many domain holders seek relief from domain registrars in attempting to attain a speedy resolution for cybersquatting claims.²⁵ This is particularly true where domain name holders are difficult to find, procedurally difficult to sue, or nonresponsive to attempted communications regarding the alleged cybersquatting.²⁶ Unfortunately, both the ACPA and the UDRP provide potential hurdles to those who seek relief from domain name registrars.²⁷

An apt illustration of this issue playing out is in *Petronas*, where a cybersquatter used GoDaddy.com as its registrar.²⁸ In 2007, a third party who had registered the names *petronastower.net* and *petronastowers.net* transferred its registration service to GoDaddy.²⁹ Using GoDaddy's name forwarding service, the third party directed web traffic from those domain names to an adult website called *camfunchat.com*.³⁰ In 2009, Petronas officials contacted GoDaddy and requested that it "take action against the website associated with the 'petronastower.net' domain name."³¹ GoDaddy conducted an investigation, but refused to take action on what was a clear cybersquatting violation because it did not host the site, and because it claimed it was prevented under the UDRP from participating in trademark disputes regarding domain name

23. *Id.*

24. *See* *Petroleum Nasional Berhad, (Petronas) v. GoDaddy.com, Inc.*, 737 F.3d 546, 548 (9th Cir. 2013).

25. *See id.*

26. *See id.* at 554.

27. *See* 15 U.S.C.A. § 1125(d) (Westlaw through Pub. L. No. 114-254); *Uniform Domain Name Dispute Resolution Policy*, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN), <https://www.icann.org/resources/pages/policy-2012-02-25-en> (last visited Aug. 31, 2016); Scaturro, *supra* note 17, at 899.

28. 737 F.3d at 548.

29. *Id.*

30. *Id.*

31. *Id.*

ownership.³² In spite of almost certain violations of the standards of the ACPA and the similar standards of the UDRP, GoDaddy did nothing. In response, Petronas sued, attempting to persuade the court to read a cause of action for contributory cybersquatting into the ACPA.³³ Despite the existence of persuasive case law in the California District Courts supporting claims for contributory cybersquatting, the Ninth Circuit Court of Appeals held that:

(1) the text of the Act does not apply to the conduct that would be actionable under such a theory; (2) Congress did not intend to implicitly include common law doctrines applicable to trademark infringement because the ACPA created a new cause of action that is distinct from traditional trademark remedies; and (3) allowing suits against registrars for contributory cybersquatting would not advance the goals of the statute.³⁴

For the reasons stated below however, it is clear that the court's analysis is not supported by analogies to the creation of contributory liability actions in trademark infringement, the legislative history, the statutory construction, or the policies that drive the statute.

II. THE HISTORY AND NATURE OF THE ACPA IMPLICITLY CREATES AN ACTION FOR CONTRIBUTORY CYBERSQUATTING

Several district courts had considered the issue of whether an action for contributory cybersquatting existed, and many had

32. *See id.* The UDRP is an alternative dispute resolution process that was adopted by ICANN in 1999. *Uniform Domain Name Dispute Resolution Policy*, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN), <https://www.icann.org/resources/pages/policy-2012-02-25-en> (last visited Aug. 31, 2016). It establishes by mandatory contractual obligation, an expedited and inexpensive arbitration process for resolving cybersquatting claims. *Id.* It also provides that registrars need only intervene in a cybersquatting dispute upon order of a court or an arbitration decision. *Id.* While certainly more efficient than a lawsuit against a cybersquatter under the ACPA, a UDRP arbitration action can take 50-60 days to resolve, a period during which the infringing website remains up and running. *Id.*; *see also* Charles Runyan, *6 Ways to Recover a Domain Name from an Infringing Cybersquatter*, DOMAIN SHERPA (last updated Dec. 9, 2015), <http://www.domainsherpa.com/6-ways-to-recover-a-domain-name-from-an-infringing-cybersquatter/>. For many trademark holders, even such a short period of time can inflict irreparable damage to their mark.

33. *Petronas*, 737 F.3d at 549-50.

34. *Id.* at 550.

answered in the affirmative.³⁵ Those courts that have applied contributory liability have relied on an analogy to *Inwood Labs, Inc. v. Ives Labs, Inc.*, a 1982 Supreme Court case that created an action for secondary liability for trademark infringement under the Lanham Act.³⁶ There, the Court considered the statute as legislated against the backdrop of common law tort liability rules, taking into account those tort principles as applied to trademark dilution actions at common law.³⁷ It reasoned that the legislature intended to incorporate those common law principles into the statute, despite the fact that neither the statute, nor the legislative history suggested that such common law principles were a consideration.³⁸

In spite of that decision, and the fact that the ACPA was created as a part of the Lanham Act, under the same umbrella of trademark protection, the *Petronas* Court dismissed the ACPA as creating a new and distinct cause of action that should not be afforded the same incorporation of broad common law tort principles.³⁹ In doing so, the court ignored the principle that “[s]tatutes 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.”⁴⁰ Instead, the court contrasted the ACPA from the Lanham Act as a whole, reasoning that, prior to the enactment of the Lanham Act, the Supreme Court had recognized

35. See, e.g., *Lockheed Martin Corp. v. Network Sols., Inc.*, 194 F.3d 980, 983 (9th Cir. 1999); *Verizon Cal., Inc. v. Above.com Pty, Ltd.*, 881 F. Supp. 2d 1173, 1181 (C.D. Cal. 2011); *Solid Host, NL v. NameCheap, Inc.*, 652 F. Supp. 2d 1092, 1112 (C.D. Cal. 2009); *Ford Motor Co. v. GreatDomains.com, Inc.*, 177 F. Supp. 2d 635, 646 (E.D. Mich. 2001).

36. 456 U.S. 844, 854 (1982) (“[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 contributorily responsible for any harm done as a result of the deceit.”). The Lanham Act codified the trademark laws that existed at its time of passing in 1946. It has then since been amended by the ACPA to add new cybersquatting causes of action. See *Petronas*, 737 F.3d at 549.

37. *Inwood Labs*, 456 U.S. at 854. See also *Meyer v. Holley*, 537 U.S. 280, 285 (2002) (“[W]hen Congress creates a tort action, it legislates against a legal background of ordinary tort-related vicarious liability rules and consequently intends its legislation to incorporate those rules.”).

38. *Inwood Labs*, 456 U.S. at 854.

39. 737 F.3d 546, 553 (9th Cir. 2013).

40. *United States v. Texas*, 507 U.S. 529, 534 (1993).

a common law theory of contributory liability into the law of trademarks and unfair competition.⁴¹ Conversely, no such common law theory had been recognized for cybersquatting.⁴² Since cybersquatting was considered a new and distinct action, the court reasoned that it should not receive the benefits of common law contributory liability.⁴³ Further, the court reasoned that since the ACPA and trademark infringement bear distinct elements—namely that trademark infringement requires commercial use by the alleged infringer, while the ACPA does not, and that the ACPA requires bad faith, while trademark infringement does not—the statutes create different rights, and thus are not entitled to the same common law incorporation.⁴⁴

This narrow view, however, does not consider the fact that, as mentioned above, prior to the enactment of the ACPA, cybersquatting type claims were litigated under traditional trademark infringement and anti-dilution claims.⁴⁵ Although no cases expressly apply or even allege contributory liability under those circumstances, presumably given the fulfillment of the elements of an infringement or unfair competition claim, a court would have applied contributory liability under that statute.⁴⁶ Indeed, even the *Petronas* Court concedes that “trademark holders may still bring claims for traditional direct or contributory trademark infringement that arises from cybersquatting activities” under 15 U.S.C. § 1125(d)(3).⁴⁷ That the legislature sought to create a more narrowly tailored law, while intentionally placing it within the Lanham Act, which until the enactment of the ACPA was implied to have incorporated contributory claims in its entirety, should not preclude it from receiving the benefits of broad tort theories of contributory liability.⁴⁸ Moreover, the fact that the cybersquatting action did not exist during the time that the common law underlying the Lanham Act was developing does not preclude it from adopting those basic principles that underlie

41. *Petronas*, 737 F.3d at 552.

42. *Id.*

43. *Id.*

44. *Id.* at 552–53.

45. Scaturro, *supra* note 17, at 883.

46. *See Petronas*, 737 F.3d at 552.

47. *Id.* at 554 (citing 15 U.S.C. § 1125(d)(3)).

48. *See Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854 (1982); S. REP. NO. 106-140, at 1 (1999).

the act as a whole. Clearly, the legislature could have thought that the ACPA was sufficiently similar to the rest of the Lanham Act to be subsumed as an amendment within it, rather than being created as a separate statutory section, and thus it is reasonably inferred that it meant for the same underlying tort principles to apply.⁴⁹ Furthermore, the distinction, which is based on differing elements, is far too narrow and arbitrary a distinction, particularly because the discrete requirements of infringement claims and defenses under the Lanham Act do not mirror their common law predecessors exactly, but are still afforded the implication of contributory liability.⁵⁰

The Ninth Circuit also concludes that the plain language of the ACPA precludes a cause of action for contributory cybersquatting.⁵¹ The court begins by invoking the canon of statutory interpretation, which requires the court to “presume that [the] legislature says in a statute what it means and means in a statute what it says there.”⁵² The court reasoned that by employing the language to impose liability on those that “register [], traffic[] in, or use[] a domain name’ with the ‘bad faith intent to profit’ from that protected mark,”⁵³ the plain language limits the circumstances under which one can be found liable for cybersquatting to those who directly commit these acts, as opposed to one who aids and abets them.⁵⁴ The court took issue with extending liability to include merely complicit registrars, whose acts were unmotivated by a bad faith intent to profit, as opposed to direct cybersquatters who demonstrated bad faith intent.⁵⁵

On its face, this does appear to be a problem. However, looking to interpretations of contributory liability for trademark infringement under the Lanham Act and adapting them in light of the bad faith requirement, the language can be reconciled. In the same way that there is no express provision in the plain language

49. See S. REP. NO. 106-140, at 1–4 (1999) (modernizing sections of the Lanham Act by including online intellectual property, such as domains, into the statutory framework).

50. See 15 U.S.C.A. § 1125(a) (Westlaw through Pub. L. No. 114–254).

51. *Petronas*, 737 F.3d at 550.

52. *Conn. Nat’l Bank v. Germain*, 503 U.S. 249, 253–54 (1992).

53. *Petronas*, 737 F.3d at 550 (quoting 15 U.S.C. § 1125(d)(1)(A)(i)–(ii) (alteration in original)).

54. *Id.* at 550–51.

55. *Id.*

of the ACPA for contributory liability, there is also no such language in the Lanham Act relating to infringement.⁵⁶ Despite the lack of direct language, the *Inwood* Court imported common law principles in determining that the contributor is liable: (1) when he “intentionally induces another to infringe on a trademark,” or (2) when he “continues to supply its product to one whom [he] knows or has reason to know is engaging in trademark infringement”⁵⁷ In order to avoid an overextension of contributory liability in light of the language of the statute, subsequent courts refined the test, particularly in *Lockheed Martin Corp. v. Network Solutions, Inc.*, which held that a defendant can be held contributorily liable only if he created a marketplace wherein infringement was occurring and he exercised a sufficient degree of control and monitoring over the infringer’s means of infringement.⁵⁸ In doing so, the court was able to import the common law tort theory into the statute, while crafting it in such a way as to avoid contradicting the statute, by including only language that almost equates to a participation in the infringement.⁵⁹

District courts have employed the same method to formulate an action for contributory cybersquatting.⁶⁰ In *Ford Motor Co. v. GreatDomains.com, Inc.*, the court determined that a plaintiff could establish a cause of action under the necessary marketplace analysis, but found that the plaintiffs in that case did not meet the high threshold set forth by the bad faith requirement.⁶¹ In importing bad faith into a contributory liability context, the court added that the “plaintiff would have to demonstrate that the ‘cyber-landlord’ knew or should have known that its vendors had no legitimate reason for having registered the disputed domain names in the first place.”⁶² The court also considered whether the contributor profited off of the use of the marketplace for

56. See generally 15 U.S.C.A. § 1125 (Westlaw through Pub. L. No. 114-254).

57. 456 U.S. 844, 854 (1982).

58. 194 F.3d 980, 984 (9th Cir. 1999). This analysis is often referred to as the “necessary market analysis.”

59. See *id.*

60. See, e.g., *Ford Motor Co. v. GreatDomains.com, Inc.*, 177 F. Supp. 2d 635, 646–47 (E.D. Mich. 2001).

61. *Id.* at 647.

62. *Id.*

cybersquatting purposes.⁶³ This high bar ensured that the plain language of the statute remained in force, while incorporating common law tort liability principles.

In spite of the practical and flexible interpretations offered by California district courts, the Ninth Circuit instead chooses to adopt an intensely narrow analysis, focusing merely on the absence of express language in the statute pointing to contributory liability.⁶⁴ In doing so, it removes the ACPA from its statutory and common law context, considering it in isolation based merely on a limited and shortsighted construction of the language of the statute. Were the same analysis applied with regard to the rest of the Lanham Act, the well settled proposition that contributory liability applies in trademark infringement suits would be entirely undermined, as it similarly lacks express language regarding contributory liability.⁶⁵ It does not make sense that a mere variation of the same statutory section would be subject to a different type of language analysis, especially where an application of the same analysis yields a result that comports perfectly well with the language of the statute, given only a slight variation based on the interpretation of good faith.

III. THE GOALS OF THE ACT SUPPORT AN ACTION FOR CONTRIBUTORY LIABILITY

The final reason that the *Petronas* Court offers for not extending contributory liability to cybersquatting is that creating such an action does not further the goals of the statute as articulated by the senate report.⁶⁶ The court points out that the statute was enacted “in order to ‘protect consumers . . . and to provide clarity in the law for trademark owners by prohibiting the bad-faith and abusive registration of distinctive marks’”⁶⁷

63. *Id.* at 648–49.

64. *Petronas*, 737 F.3d at 551.

65. *See generally* 15 U.S.C.A. § 1114 (Westlaw through Pub. L. No. 114-254).

66. *Petronas*, 737 F.3d at 553–54; *see* S. REP. NO. 106–140, at 4, 7–9 (1999) (the senate report specifically outlines the purpose and analysis of the statute’s enactment, and notably never raises nor discusses the idea of contributory liability).

67. *Petronas*, 737 F.3d at 553 (quoting S. REP. NO. 106-140, at 4). “The purpose of the bill is 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

The court also focuses on the statutory provision which states:

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, the bill does not extend to innocent domain name registrations by those who are unaware of another's use of the name, or even to someone who is aware of 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.⁶⁸

The court construes this purpose as an intention to impose a strict limitation “on who can be liable for cybersquatting and in what circumstances.”⁶⁹ While this may be true, a construction of the statute which requires the “exceptional circumstances” contemplated by *GreatDomains*, creates a similar limitation, focusing more on the conduct of the defendants rather than their degree of participation relative to the actual cybersquatting.⁷⁰ The limitation is assuredly narrow, shielding domain name registrars who register cybersquatters merely as an oversight, while really only applying to the types of scenarios where, like in *Petronas*, the registrar is informed of a particularly egregious case of cybersquatting, and the registrar does nothing while it continues to derive additional revenue from services such as redirecting and hosting.⁷¹ *Petronas* also alludes to, as other authors have likewise noted, that there was an additional Congressional intent to limit the scope of the ACPA so as “to ensure that any remedies do not impede or stifle the free flow of information on the Internet.”⁷²

There are several concerns that might be raised. First,

distinctive marks as Internet domain names with the intent to profit from the goodwill associated with such marks—a practice commonly referred to as ‘cybersquatting.’” S. REP. NO. 106–140, at 4.

68. S. REP. NO. 106–140, at 12–13; see *Petronas*, 737 F.3d at 553.

69. *Petronas*, 737 F.3d at 553.

70. *Ford Motor Co. v. GreatDomains.com, Inc.*, 177 F. Supp. 2d 635, 647 (E.D. Mich. 2001).

71. See *id.*; *Petronas*, 737 F.3d at 548.

72. Walczak, *supra* note 5, at 556; see *Petronas*, 737 F.3d at 553–54.

creating contributory liability might force domain name registrars to make a determination as to bad faith prior to registering a domain name, thus slowing down the registration process.⁷³ Next, registrars might have to monitor domain names more closely, which is extremely difficult given the number of domains companies like GoDaddy maintain.⁷⁴ Finally, “imposing contributory liability for cybersquatting would incentivize ‘false positives,’ in which the lawful use of a domain name is restricted by a risk-averse third party service provider that receives a seemingly valid take-down request from a trademark holder.”⁷⁵

While these concerns have a degree of validity to them, it is important to consider them in practice, and also to consider the countervailing policy issues that result when the government fails to hold registrars accountable. First, as mentioned above, under the type of high bar set forth in *GreatDomains*, finding contributory liability would be a rare occurrence, extending to those circumstances where registrars exercised a degree of control greater than a mere one-time registration, or where registrars had actual or constructive knowledge of blatant cybersquatting activities.⁷⁶ The statute as interpreted does not target those innocent parties contemplated by the senate report, and instead targets those who demonstrate a reckless complicity in cybersquatting activity.⁷⁷ Rooting out these types of users is likely not as difficult as one might think. Dissidents lament that registrars will be forced to conduct the nine-part test that the ACPA statute sets out for determining bad faith, which they claim would be a nearly impossible task.⁷⁸ However, the statute as interpreted by the modified necessary market analysis in *GreatDomains* does not require such a meticulous review and monitoring of domains, merely that the registrar take notice of the activities of domains over which it has a significant degree of control, and where registrants have no legitimate reason for

73. Walczak, *supra* note 5, at 556.

74. *Id.*

75. *Petronas*, 737 F.3d at 553.

76. *Ford Motor Co. v. GreatDomains.com, Inc.*, 177 F. Supp. 2d 635, 647 (E.D. Mich. 2001).

77. *See id.* at 641–42.

78. *Petronas*, 737 F.3d at 553. The referenced statute pertains to 15 U.S.C. § 1125(d)(1)(B) and the statute’s non-exhaustive nine-factor test that the statute lays out to help determine whether a person has acted in bad faith. *Id.*

having registered the disputed domain names to begin with.⁷⁹ Thus, the registrars would only have to conduct such an analysis in a limited number of scenarios, such as the one in *Petronas*, where GoDaddy provided hosting and forwarding services to the cybersquatter, the domain name mirrored exactly the trademarked name of a large corporation, and GoDaddy was notified of the cybersquatting.⁸⁰

Whatever inconvenience additional monitoring creates for the massive companies that register domain names will likely be far outweighed by the benefit received by trademark holders who benefit from incentivized registrars that are more proactive about preventing cybersquatting before it starts.⁸¹ Trademark holders who have clear rights to a domain name will also have the option to get quick relief from potentially dangerous redirecting or pirating merely by notifying registrars of potential cybersquatting, which triggers the duty of the registrars to stamp out egregious case while not forcing them to preemptively shut down closer calls and allowing the UDRP provisions to kick in.⁸² In sum, an interpretation of the ACPA that creates an action for contributory liability best serves the policy goals surrounding the intent of the ACPA by providing more efficient and robust protection of trademark rights, while setting a high enough bar to prevent registrars from being forced to slow down the registration process due to the need to conduct onerous reviews of every domain name they register.

IV. CONCLUSION

Like the rapid changes that the internet has undergone since the creation of the ACPA in 1999, the problems arising from cybersquatting are constantly changing.⁸³ To effectively police

79. See *GreatDomains*, 177 F. Supp. 2d at 647.

80. See *Petronas*, 737 F.3d at 548.

81. *Contra* Walczak, *supra* note 5, at 556–57 (proposing that the costs outweigh the benefits of enforcing contributory liability in ACPA cases).

82. *But see* *Petronas*, 737 F.3d at 548–49. In *Petronas*, the court found secondary liability could not be applied, and thus the registrar could not be found liable for its mere inaction. *Id.* The purpose of allowing secondary liability to apply in this context is to force a registrar to act in order to protect itself from liability. Such action, however, is what will further protect a rightful trademark owner.

83. *Changing with the cybersquatters: the evolution of brand protection*, WORLD TRADEMARK REV. BLOG (Sept. 3, 2012), <http://www.worldtrademark>

cybersquatting, it is necessary to broadly interpret and flexibly apply the ACPA. Rigid interpretations, like the one employed in *Petronas*, allow cybersquatters to insulate themselves from efficient repercussions by dodging and dragging out lawsuits and arbitration, while also allowing registrars to disclaim responsibility of complicity in obvious cybersquatting ordeals.⁸⁴ By interpreting the ACPA against the backdrop of common law vicarious liability principles, in the same way courts have interpreted trademark infringement under the Lanham Act, courts can effectively deter registrars from turning a blind eye to cybersquatting and allow trademark holders to obtain relief from those who hold the greatest amount of control over domain names, and who are in the best position to prevent it from the outset, given only a small amount of oversight.⁸⁵ Allowing contributory liability actions against domain name registrars also offers greater potential for the actual recovery of damages where harm to a mark is done, and targets litigation against parties who will be more willing to quickly take down infringing names in an efficient manner.⁸⁶ Thus, the potential for contributory liability is likely to have the effect of reducing litigation, rather than increasing it, and promoting efficient internet commerce. Because of this effect, courts can fulfill the goals of the statute while staying within its powers to interpret it. Accordingly, if and when another case reaches the Supreme Court, the Court should follow the rationale of its prior decision in *Inwood* and firmly establish an action for contributory liability under the ACPA.⁸⁷

review.com/log/detail.aspx?g=5d4d92f6-5a20-4779-9e7b-0cd1afa1ad8e.

84. See *Petronas*, 737 F.3d at 550; Brenda R. Sharton, *Domain Name Disputes: To Sue or Not To Sue*, Bos. B.J., Sept.–Oct. 2000, at 10 (for the proposition that ACPA “include[s] traditional claims of trademark infringement”).

85. See *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854–55 (1982).

86. See *Changing with the cybersquatters: the evolution of brand protection*, *supra* note 83 (for the proposition that it can be very difficult to locate and pinpoint the exact registrant responsible for cybersquatting because of the international reach of the internet and sophisticated tactics used to dodge liability).

87. See 456 U.S. at 854–55.