

A *Barcelona.com* Analysis: Toward a Better Model for Adjudication of International Domain Name Disputes

Zohar Efroni*

INTRODUCTION	31
I. INTRODUCTION TO INTERNATIONAL DOMAIN NAME DISPUTES	32
<i>A. Internet and Domain Names Architecture</i>	32
<i>B. Introduction to Territorial Jurisdictional Issues</i>	34
1. In Personam Jurisdiction	35
2. In Rem Jurisdiction	39
<i>C. The Intersection of Trademark Law and Domain Name Disputes</i>	41
1. The Basic Tension	41
2. The Prehistory of Cybersquatting Regulation	43
II. THE NEW LEGAL FRAMEWORK	48
<i>A. The UDRP</i>	48
1. The UDRP Mechanism in Brief	48
2. The Mutual Jurisdiction Problem and Rule 3(b)(xiii)	52
<i>B. The ACPA</i>	53
1. In Personam Action	54
2. In Rem Action	55
3. The Reverse Domain Name Highjacking Provision	57
III. THE <i>BARCELONA.COM</i> DISPUTE	63
<i>A. The Facts</i>	64

* L.L.B., L.L.M. This piece is dedicated to my family, Sarah and Lian.

<i>B. The Forth Circuit Ruling</i>	66
1. Jurisdictional Issues.....	66
2. Foreign Law Not Applicable.....	68
3. The Elements of the RDNH Provision.....	68
4. BARCELONA Is Not a Protected Mark in the United States.....	69
IV. ANALYSIS AND PROBLEMS IN THE PRESENT STATE OF THE LAW.....	69
<i>A. Correct Application of the Law</i>	70
<i>B. The Territoriality Argument</i>	71
<i>C. Emerging Litigation Strategies</i>	73
1. The Registrant's (Probably) Winning Strategy.....	74
2. The Foreign-Mark Owner's (Probably) Losing Strategy.....	77
3. The Partial Reverse Effect.....	78
<i>D. The Big Picture and Its Critique</i>	79
1. Minimum Contacts Yes or No; What Does <i>Shaffer</i> Really Mean?.....	79
2. The Extraterritorial Effect of the ACPA.....	81
3. International Comity Considerations.....	84
4. The ACPA Laundry Machine Effect and Its Paradox.....	86
<i>E. Possible Foreign Reactions</i>	89
V. A PROPOSAL FOR A BETTER MODEL: THE INTERNATIONAL ANTICYBERSQUATTING TREATY.....	91
<i>A. Unilateral Approach: A Lose-Lose Situation</i>	92
<i>B. Possible Solution: The IACT</i>	95
<i>C. Testing the Model</i>	100
1. Applying <i>Barcelona.com</i> in an IACT Legal Framework.....	100
2. The Game Theory Model.....	102
a) The Post- <i>Barcelona.com</i> World.....	104
i. Explanation	105
ii. Analysis	108
b) The IACT World.....	109
i. Explanation	109
ii. Analysis	110

2003]	<i>BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES</i>	31
	<i>D. Why Should the IACT Be Attractive to Internet Nations?</i>	113
	1. Everyone Gets a Slice of the Pie	113
	2. IACT Critique.....	114
	CONCLUSION.....	116

INTRODUCTION

The terms “cybersquatting,” “ACPA,” “UDRP,” and “reverse domain name hijacking” are becoming less obscure and esoteric and are not longer restricted to professional jargon used solely by Internet and trademark law specialists. In the last few years, numerous news and magazine articles, as well as professional and academic publications, introduced the phenomenon of cybersquatting, described the tools formulated to combat it and touched upon some problematic aspect in this rapidly developing field. This Article analyzes one of the most concerning aspects of U.S. cybersquatting law: foreign actors litigating domain name disputes in U.S. federal courts. This problem surfaced and received special attention in the Fourth Circuit’s recent decision in *Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona*.¹

Part I of this Article provides essential background to domain name dispute issues. Part II describes the legal framework created to deal with cybersquatting activities, namely the Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy. Part III provides an overview on the background and facts surrounding the *Barcelona.com* domain name dispute and the Fourth Circuit’s ruling. Part IV consists of a critical analysis of the decision and discussion of its resulting troublesome consequences. Finally, Part V presents an alternative to current cybersquatting policy and approaches. In addition, it provides a new model that highlights the advantages of the alternative as compared with the shortcomings of the present approaches.

¹ 330 F.3d 617 (4th Cir. 2003).

I. INTRODUCTION TO INTERNATIONAL DOMAIN NAME DISPUTES

A discussion of the issues raised by international domain name disputes requires some background knowledge about the Internet and the law that affects it. Along with a cursory overview on the Internet and domain name structure, this part includes an introduction to the relevant jurisdictional issues, a discussion of the tension between domain name rules and trademark law, and a survey of the pre-regulation landscape.

A. *Internet and Domain Names Architecture*

The Internet is a giant “network of networks” facilitating communication and information transfer between the millions of computers connected to it.² The domain name system (“DNS”), the addressing mechanism of the Internet, is designed in a hierarchal structure.³ Internet addresses consist of alphanumeric strings separated by a dot (.), e.g., <news.google.com>, and are read from left (the lower level of the domain) to right (the higher level of the domain).⁴ Theoretically, there is a highest-level domain at the apex of the domain name space, the “root domain,” which is usually left unnamed, under which all domains fall.⁵

Below the root domain are top-level domains (“TLDs”), which are the highest level of named domains and the part of the address to the extreme right.⁶ Top-level domains, in turn, are divided into two major categories:⁷ generic top-level domains (“gTLDs”) and

² For a detailed explanation of the Internet, see *ACLU v. Reno*, 929 F. Supp. 824, 830–38 (E.D. Pa. 1996), *aff’d*, 521 U.S. 844 (1997).

³ The domain name system (“DNS”) basically correlates the numerical IP addresses assigned to all computers or “hosts” connected to the Internet (addresses that can be recognized by computers) and alphabetical strings of characters entered into the search tool in the user’s browser (addresses that can be more easily remembered by users). For a description of the DNS, see Orion Armon, *Is This as Good as It Gets? An Appraisal of ICANN’s Uniform Domain Name Dispute Resolution Policy (UDRP) Three Years After Implementation*, 22 REV. LITIG. 99, 101–03 (2003).

⁴ See Kim G. von Arx & Gregory R. Hagen, *Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control*, 9 RICH. J.L. & TECH. 4, ¶ 11 (2002), at <http://www.law.richmond.edu/jolt/v9i1/article4.html>.

⁵ *Id.*

⁶ See *id.* ¶ 12.

⁷ A third category of top level domains (“TLDs”) is an infrastructure TLD (“iTLD”) called <.arpa>, which is used solely for Internet infrastructure purposes. See *id.* ¶ 12.

country-code top-level domains (“ccTLDs”).⁸ Thus, in the domain name <www.yahoo.com>, the top-level domain is <.com>. The string of characters <yahoo> is the second-level domain (“SLD”) registered in the top-level registry <.com> file zone.⁹

Those TLD servers catalogue domain names registered under all the ccTLDs and gTLDs.¹⁰ The TLD servers communicate with other servers containing second-level registrations such as <yahoo>. In fact, there is no single computer containing the entire database of all domain names, since the TLD servers are located in “myriad locations worldwide.”¹¹

In the 1980s, seven gTLDs were introduced,¹² three of which could be registered without restrictions (<.com>, <.net>, and <.org>).¹³ Later, four additional non-restricted gTLDs were created (<.biz>, <.info>, <.name>, and <.pro>).¹⁴ Presently, six of

⁸ See Colby B. Springer, *Master of the Domain (Name): A History of Domain Name Litigation and the Emergence of the Cybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy*, 17 SANTA CLARA COMPUTER & HIGH TECH L.J. 315, 320–23 (2001) (explaining the TLD structure and registration procedure).

⁹ Every generic TLD (“gTLD”) has only one registry. A registry is the entity that stores, manages, and maintains the entire list of second level domains (“SLDs”) registered under that gTLD. The registry is also responsible for licensing commercial registrars, which sell available SLDs to consumers. See *Cable News Network, LP v. CNNNews.com*, 162 F. Supp. 2d 484, 486 n.4 (E.D. Va. 2001) [hereinafter *CNN I*], *vacated in part on other grounds by Cable News Network, LP v. CNNNews.com*, No. 02-1112, 2003 WL 152846 (4th Cir. Jan. 23, 2003) [hereinafter *CNN Appeal*]; see also Tamar Frankel, *The Managing Lawmaker In Cyberspace: A Power Model*, 27 BROOK. J. INT’L L. 859, 870–71 (2002) (describing the hierarchal structure of the DNS).

¹⁰ Armon, *supra* note 3, at 102 (describing the hierarchy of the root servers, TLD servers and sub-level domain directories).

¹¹ See Catherine T. Struve & R. Polk Wagner, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 17 BERKELEY TECH. L.J. 989, 1019 (2002).

¹² These gTLDs were: <.com>, <.edu>, <.gov>, <.int>, <.mil>, <.net>, and <.org>. See ICANN, *Top-Level Domains*, at <http://www.icann.org/tlds> (last visited Oct. 30, 2003) [hereinafter *Top-Level Domains*].

¹³ *Id.* Unrestricted gTLDs are ones that are not restricted to certain institutions or subjects. Examples of restricted gTLDs are <.gov> (restricted to the U.S. government), <.edu> (restricted to academic institutions), and <.mil> (restricted to the U.S. military). See Armon, *supra* note 3, at 103–04.

¹⁴ See *Top-Level Domains, supra* note 12.

these seven gTLD registries are physically located in U.S. territory.¹⁵

The Internet Corporation for Assigned Names and Numbers (“ICANN”), a not-for-profit organization, is responsible for the maintenance and management of the gTLD directories by virtue of an exclusive contract with the U.S. government.¹⁶ The administration of the ccTLD registries such as <.ca> for Canada, <.fr> for France, and <.uk> for the United Kingdom, however, is “controlled by the corresponding national government[s].”¹⁷

B. Introduction to Territorial¹⁸ Jurisdictional Issues

In the context of international jurisdictional law, it is useful to distinguish between three types of jurisdictional powers: jurisdiction to prescribe (sometimes called legislative jurisdiction),¹⁹ jurisdiction to adjudicate (sometimes called judicial

¹⁵ *Id.* It appears that the <.name> registry, based in London, is the only registry located outside of the United States. See Global Name Registry, at <http://www.nic.name> (last visited Oct. 30, 2003) (official Web site of the <.name> registry).

¹⁶ See A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 50–93 (2000) (describing the contractual relationship between the U.S. government and the Internet Corporation for Assigned Names and Numbers (“ICANN”) and providing detailed background on the creation and functions of ICANN); see also Katherine Meyers, Note, *Domain Name Dispute Resolution in U.S. Courts: Should ICANN Be Given Deference?*, 43 B.C. L. REV. 1177, 1183–86 (2002) (describing the functions of ICANN).

¹⁷ See Lisa M. Sharrock, Note, *The Future of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions from Within the UDRP Framework*, 51 DUKE L.J. 817, 840–01 (2001) (noting that unlike domain names with generic TLDs, administration of each country code TLD (“ccTLD”) is controlled by the corresponding national government); see also von Arx & Hagen, *supra* note 4, ¶ 20 (noting that the U.S. government policy was to give national governments authority to manage or establish policy for their own ccTLDs).

¹⁸ In rem and in personam jurisdictions are sometimes categorized as “territorial jurisdictions,” as distinguished from subject matter jurisdiction. “For a person or property to be subject to a particular court’s jurisdiction, there must be a proper connection between the person or property and the sovereign state in whose name the court acts.” *FleetBoston Fin. Corp. v. FleetBostonFinancial.com*, 138 F. Supp. 2d 121, 129 (D. Mass. 2001) (citing 16 MOORE’S FEDERAL PRACTICE § 108.01 (Matthew Bender 3d ed.)). The terms personal jurisdiction and in personam jurisdiction are used interchangeably in this Article.

¹⁹ Jurisdiction to prescribe is a state’s authority to make its laws applicable to the “activities, relations, or status of persons, or the interests of persons in things”

jurisdiction),²⁰ and jurisdiction to enforce (sometimes called executive jurisdiction).²¹ The power and authority of a state to legislate, adjudicate, and enforce its national law in the international sphere are traditionally subject to constraints of territoriality, nationality, and effect.²² Thus, every state has the obligation to exercise moderation and restraint in invoking jurisdiction over cases involving foreign elements.²³ The Internet, providing a global and border-free platform for communication, information, and various commercial activities, challenges traditional concepts of jurisdiction.

1. In Personam Jurisdiction²⁴

Since in personam jurisdiction determines when a defendant is subject to adjudicative process of the court, it is closely related to the judicial jurisdiction concept and its general limitations. The rule in any inquiry into whether a state can subject a person or a thing²⁵ to the process of its courts is the rule of “reasonableness.”²⁶

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(a) (1986) [hereinafter RESTATEMENT OF FOREIGN RELATIONS LAW].

²⁰ Jurisdiction to adjudicate is a state’s authority “to subject persons or things to the process of its courts or administrative tribunals . . .” *Id.* § 401(b).

²¹ Jurisdiction to enforce is a state’s authority “to induce or compel compliance or to punish noncompliance with its laws or regulations . . .” *Id.* § 401(c).

²² *Id.* § 401 cmt. a (noting that a state’s different jurisdictional powers each have different limitations under international law); *see also* Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117 (Dec. 1997) (describing the application of international law principles on jurisdictional concepts), *available at* <http://www.law.indiana.edu/fclj/pubs/v50/no1/wilske.html> (last visited Nov. 19, 2003).

²³ *See Asahi Metal Indus. Co. v. Super. Ct. of Calif.*, 480 U.S. 102, 115 (1987) (“Great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field.” (quoting *United States v. First Nat’l City Bank*, 379 U.S. 378, 404 (1965) (Harlan, J., dissenting))).

²⁴ This overview of in personam jurisdiction is based on material in a previous article by this author. *See* Zohar Efroni, *The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: New Opportunities for International Forum Shopping?*, 26 COLUM.-VLA J.L. & ARTS 335, 339–41 (2003).

²⁵ This rule is also relevant to in rem jurisdiction. *See infra* Part I.B.2 (discussing principles of in rem jurisdiction).

²⁶ “A state may exercise jurisdiction through its courts to adjudicate with respect to a person or thing if the relationship of the state to the person or thing is such as to make the exercise of jurisdiction reasonable.” RESTATEMENT OF FOREIGN RELATIONS LAW, *supra* note 19, § 421(1).

U.S. courts,²⁷ considering whether to assert personal jurisdiction, generally look at two elements: the long-arm statute in the jurisdiction at issue and the due process requirement of the U.S. Constitution.²⁸ Personal jurisdiction may be divided into two types: general jurisdiction and specific jurisdiction. General jurisdiction is applicable when the defendant has engaged in “‘systematic and continuous activities’ in the forum state.”²⁹ In this instance, the plaintiff does not have to show a connection between the forum-related activities of the foreign party and the cause of action.

In the context of jurisdiction arising out of online activity, the systematic and continuous contacts are often absent. Specific jurisdiction, however, which does not require systematic and continuous contacts, may apply if the cause of action is related to the foreign party’s activity in the forum state. The power to assert personal jurisdiction, however, was discussed in *Asahi Metal Industry Co. v. Superior Court of California*.³⁰ Justice O’Connor’s plurality opinion in the *Asahi* case stated that a court could subject a corporation to suit in a state only if the defendant took an action “purposefully directed” toward the forum state.³¹ The mere placement of a product into the stream of commerce, without more, is not such an act; the defendant must take additional action to indicate the “intent or purpose to serve the market in the forum state”—advertising, for example.³²

²⁷ Most of the cases described in this subsection decided domestic U.S. disputes, in which the question was which U.S. state had personal jurisdiction over a defendant. U.S. personal jurisdiction concepts, however, are also applicable to international disputes.

²⁸ See *Kulko v. Super. Ct. of Calif.*, 436 U.S. 84, 91 (1978) (stating that personal jurisdiction depends upon the presence of reasonable notice to the defendant that an action has been brought and a sufficient connection between the defendant and the forum state to make it fair to require defense of the action in the forum).

²⁹ *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1122 (W.D. Pa. 1997) (citing *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 414–16 (1984)).

³⁰ 480 U.S. 102 (1987).

³¹ *Asahi*, 480 U.S. at 112.

³² *Id.* The Supreme Court, however, has not yet resolved this issue. See *id.* at 116–21 (Brennan, J., concurring) (arguing against the “purposeful availment” requirement). Thus, in the Internet context, the applicable threshold for on-line activity that establishes personal jurisdiction was not definitively determined in the *Asahi* decision.

Generally, courts apply a three-prong test for asserting specific jurisdiction. The plaintiff must show that: (1) the defendant purposefully availed himself or herself of the privileges and liabilities of the jurisdictions by conducting activities specific to the jurisdiction,³³ which is a version of the traditional “minimum contacts” test;³⁴ (2) the cause of action arises from those activities;³⁵ and (3) the assertion of jurisdiction is reasonable in the circumstances.³⁶

The first prong of this test is the hardest to clarify in the context of online activities. Courts were generally reluctant to extend personal jurisdiction merely because the defendant operated a Web site that was accessible from the forum state. In this context, courts tended to follow Justice O’Connor’s opinion in *Asahi*.³⁷ Consequently, a sliding scale was developed, providing that the more commercially oriented the Web site is and the more it is engaged in direct commercial activities targeting the forum state, the more the defendant is susceptible to the forum state’s jurisdiction.³⁸ The two ends of the sliding scale proved relatively easy to identify. On one end, a purely passive Web site generally would not establish personal jurisdiction.³⁹ If a defendant was “doing business” through the Web site with individuals in the

³³ *Hanson v. Denckla*, 357 U.S. 235, 253 (1958). The test was later articulated in *Asahi*, 480 U.S. at 112.

³⁴ The “minimum contacts” test was first established in *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

³⁵ *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 472 (1985).

³⁶ See *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 416 (9th Cir. 1997) (citing *Ballard v. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995)). The role of the reasonableness as a balancing factor is explained in *Burger King*, 471 U.S. at 477.

³⁷ See, e.g., *Cybersell*, 130 F.3d at 418; *Bensusan Rest. Corp. v. King*, 937 F. Supp. 295, 301 (S.D.N.Y. 1996), *aff’d*, 126 F.3d 25 (2d Cir. 1997).

³⁸ See *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (“[O]ur review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles.” (footnote omitted)).

³⁹ A typical example was *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295, 297 (S.D.N.Y. 1996), in which the Web site contained only general informative text about the Blue Note club in Missouri, and the famous Blue Note jazz club in New York claimed infringement.

forum state, however, courts were generally willing to assert jurisdiction.⁴⁰ The difficult cases lay in the middle, cases in which the Web site was interactive but still did not amount to clearly doing business with the forum state. Some courts demanded a certain threshold of interactivity and “something more” than mere advertising in order to establish jurisdiction.⁴¹ Other courts considered whether to extend their jurisdictional reach based on the totality of contacts of defendant with the forum state, with and without regard to the Internet activities.⁴²

Recently, courts have started using an additional tool to expand personal jurisdiction in Internet-related activities known as the “effects doctrine.” The three basic components of the doctrine, which grants the forum state jurisdiction over a foreign actor, are: (1) an intentional action, (2) which is expressly aimed toward the forum-state’s jurisdiction, (3) causing harm that occurred in that jurisdiction when that actor knew it might occur.⁴³ Examples of applying this test to online activities can be found mostly in Internet-based defamation cases⁴⁴ and in cases decided before the ACPA’s enactment,⁴⁵ in which proving “purposeful availment” by the defendant was problematic.

Undoubtedly, the increase in activities—commercial and otherwise—on the Internet introduced new and difficult questions

⁴⁰ See, e.g., *CompuServe, Inc. v. Patterson*, 89 F.3d 1257, 1265–66 (6th Cir. 1996) (asserting jurisdiction on a Texas defendant, whose contacts with the forum state consisted almost exclusively of selling software through computer transmissions to CompuServe’s system in Ohio).

⁴¹ See, e.g., *Millennium Enters. v. Millennium Music, L.P.*, 33 F. Supp. 2d 907, 920–23 (D. Or. 1999) (introducing the requirement of a “deliberate action” in the forum state).

⁴² See, e.g., *Blumenthal v. Drudge*, 992 F. Supp. 44, 56–57 (D.D.C. 1998).

⁴³ See *Calder v. Jones*, 465 U.S. 783, 788–89 (1984) (establishing an “effects” test for intentional action aimed at the forum state).

⁴⁴ See, e.g., *Bochan v. La Fontaine*, 68 F. Supp. 2d 692 (E.D. Va. 1999). In *Bochan*, a Virginia resident brought an Internet defamation lawsuit in the Eastern District of Virginia against residents of Texas and Missouri. *Id.* at 694–95. Denying the defendants’ jurisdictional challenge to the court’s jurisdiction, the court stated that “because the predominant ‘effects’ of the La Fontaines’ and Harris’s conduct are in Virginia, these defendants could reasonably foresee being haled into court in this jurisdiction.” *Id.* at 702 (quoting *Calder*, 465 U.S. at 789–90).

⁴⁵ See *Panavision Int’l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998) (applying the “effects doctrine” in a classic pre-Anticybersquatting Consumer Protection Act (“ACPA”) cybersquatting case).

for U.S. courts deciding personal jurisdiction issues. The tests applied and the results that followed differed from case to case depending, *inter alia*, on the specific long-arm statute involved and each court's interpretation of the concepts of "purposeful availment" and "interactive online activity" sufficient for exercising personal jurisdiction.⁴⁶ For purposes of this Article, however, it is important to be aware of the new problems encountered by plaintiffs attempting to hail into court cyber-defendants and the potential expansion of personal jurisdiction when the allegedly unlawful act occurred "everywhere and nowhere at the same time."⁴⁷

2. In Rem Jurisdiction

In rem jurisdiction facilitates legal action against the thing (or the res) itself,⁴⁸ with legal actions commenced in the judicial situs where the thing is located.⁴⁹ Hence, the application of the rule of "reasonableness" in this context requires the res to be located in the territorial jurisdiction of the court and to have some relevancy to the dispute.⁵⁰ The three types⁵¹ of in rem jurisdictions are: (1)

⁴⁶ As of today, there is no ruling by the Supreme Court that resolves the different approaches of several circuits regarding certain questions of personal jurisdiction. See Springer, *supra* note 8, at 334.

⁴⁷ See Ira S. Nathenson, Comment, *Showdown at the Domain Name Corral: Property Rights and Personal Jurisdiction over Squatters, Poachers and Other Parasites*, 58 U. PITT. L. REV. 911, 935-46 (1997) (describing the difficulties of asserting jurisdiction in Internet-related activities).

⁴⁸ In rem is defined as "in or against the thing." BRYAN A. GARNER, A DICTIONARY OF MODERN LEGAL USAGE 453 (2d ed. 1990).

⁴⁹ "In rem jurisdiction is predicated on the notion that the res is found within the territorial jurisdiction of the court." *FleetBoston Fin. Corp. v. FleetBostonFinancial.com*, 138 F. Supp. 2d 121, 135 (D. Mass. 2001).

⁵⁰ One court explained:

In order for a court to act with authority to hear a dispute and render a judgment that will justify recognition, the court must have jurisdiction not only over the subject matter of the suit, but also over the person or property to whom or which the court's judgment will extend For a person or property to be amenable to a particular court's jurisdiction, there must be a *proper connection* between the person or property and the sovereign in whose name the court acts.

Id. at 129 (emphasis added) (citations omitted).

⁵¹ *Id.* at 132 (citing *Hanson v. Denckla*, 357 U.S. 235, 246 n.12 (1958) (noting the three types of in rem jurisdiction)); see also RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 222 topic 2 (1971).

true in rem, which arises when courts adjudicate property rights over the thing *vis-à-vis* the world;⁵² (2) quasi in rem I, in which property rights are allocated as against particular named persons;⁵³ and (3) quasi in rem II, which concerns the rights of a particular person or persons in a thing, but is distinguishable from quasi in rem I because the claim giving rise to the action “is not related to the res that provides jurisdiction.”⁵⁴

In making these distinctions, a continuing source of controversy is the Supreme Court’s 1977 decision in *Shaffer v. Heitner*.⁵⁵ The *Shaffer* court held that the mere statutory presence of a defendant’s property in a state—without any other ties among the defendant, the state, and the litigation—could not support jurisdiction over the defendants in that state.⁵⁶ Some courts believe that *Shaffer* requires minimum contacts analysis in exercising any type of in rem jurisdiction,⁵⁷ while other courts interpreted *Shaffer* as compelling such a test only in quasi in rem II cases.⁵⁸

This somewhat obscure issue regained new, fascinating life in the context of domain names. In rem jurisdiction could be an effective response to evasive cybersquatters avoiding personal jurisdiction, but the prospect of invoking in rem jurisdiction raises some difficult questions. For instance, do domain names constitute

⁵² *Hanson*, 357 U.S. at 246 n.12.

⁵³ See *Fleetboston*, 138 F. Supp. 2d at 132. Examples include actions to remove a cloud on title to land or actions seeking to quiet title against a particular rival’s claim. *Id.*

⁵⁴ *Id.* In a quasi in rem II action, “the plaintiff does not dispute the property rights of the owner of the res, but seeks to obtain the res in satisfaction of some separate claim.” *Id.*

⁵⁵ 433 U.S. 186 (1977).

⁵⁶ See *id.* at 209.

⁵⁷ For instance, the district court in *Fleetboston*, 138 F. Supp. 2d at 134, found that the *Shaffer* holding is not limited to quasi in rem type II actions:

The logic of *Shaffer*’s limitations would appear to extend to actions in which the existence of the property in the state cannot fairly be said to represent meaningful contacts between the forum state, the defendant, and the litigation. While this will generally be type II quasi in rem actions, it will not be so exclusively.

Id.

⁵⁸ See, e.g., *CNN I*, 162 F. Supp. 2d 484, 489–92 (E.D. Va. 2001) (adopting a limited reading of *Shaffer* and citing many other authorities supporting this interpretation), *aff’d in relevant part by CNN Appeal*, No. 02-1112, 2003 WL 152846 (4th Cir. Jan. 23, 2003).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 41

the necessary *res* to qualify for in rem jurisdiction? If yes, in which territory do they “exist”? Also, are minimum contacts with the forum required for exercising such jurisdiction?⁵⁹

C. *The Intersection of Trademark Law and Domain Name Disputes*⁶⁰

The friction between trademark law and domain names is a well-acknowledged problem and an inevitable outgrowth of the Internet and particularly of online commercial activities. The clash mainly arises because traditional trademark law was not designed and did not contemplate, *ab initio*, trademark disputes occurring purely in a global, electronic medium such as the Internet. In particular, the uniqueness and global reach of domain names serve to complicate the application of traditional trademark concepts.

1. The Basic Tension

When the use of marks incorporated in domain names increased through the 1990s as a tool of mark owners to promote their commercial activities, the basic tension between trademark law and domain names surfaced and intensified. There are two parts to this problem. First, there is similarity between marks and domain names as potential identifiers with the capacity to distinguish between sources of goods and services. Second, the nature and purpose of trademarks and domain names is conceptually different. As a branch of commercial competition law, trademark protection—at least under U.S. law—is primarily designed to facilitate distinctions between sources of goods or services in order to prevent confusion among consumers and to protect the goodwill of the mark.⁶¹ Conversely, the domain name

⁵⁹ See discussion *infra* Part II.B.2.

⁶⁰ The discussion about the conflict between trademark and domain name concepts is based on material included in a previous article by the author. See Efroni, *supra* note 24, at 342–46.

⁶¹ See *Avery Dennison Corp. v. Sumpton*, 189 F.3d 868, 873 (9th Cir. 1999) (“Two goals of trademark law are reflected in the federal scheme. On the one hand, the law seeks to protect consumers who have formed particular associations with a mark. On the other hand, trademark law seeks to protect the investment in a mark made by the owner.” (citing *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, 163–64 (1995))); see also 74 AM. JUR. 2D *Trademarks and Tradenames* § 1 (2001) (“The purpose of trademark law is

system was merely meant to coordinate easy-to-remember strings of letters and hard-to-memorize strings of numbers. Domain names were not meant to function as trademarks; they were thought to be simply a feature in the system of addresses corresponding with “locations” in cyberspace.⁶²

Trademark law, however, is designed both to protect the goodwill of the mark and to prevent consumer confusion.⁶³ Therefore, identical or similar marks may generally coexist for different classes of goods and services under the assumption that there is no danger of confusion.⁶⁴ Moreover, because trademark law is territorial,⁶⁵ the mark may be protected only in the sovereign giving effect to the mark, generally after determination that the mark qualifies as an identifier of goods and/or services within the territory of that sovereign.⁶⁶ Thus, trademark law can conceptually tolerate identical or similar marks in different territories within the same classes of goods and services, typically according to separate

to protect the public from confusion regarding the sources of goods or services and to protect business from the diversion of trade through the misrepresentation or appropriation of another’s goodwill.” (citing *Minneapolis Co. v. Normandin*, 338 N.W.2d 18, 22 (Minn. 1983))).

⁶² See Assafa Endeshaw, *The Threat of Domain Names to the Trademark System*, 3 J. WORLD INTELL. PROP. 323, 323 (2000) (“The initial purpose of domain names was to assign a unique address to a computer connected to a network.”).

⁶³ See, e.g., *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495 (2d Cir. 1961) (outlining a series of nonexclusive factors likely to be relevant in determining the likelihood of confusion).

⁶⁴ A major exception is famous marks. The Lanham Act protects famous marks against dilution of the distinctive quality of the mark. See 15 U.S.C. § 1125(c) (2000). Dilution is defined as “lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of . . . [the] likelihood of confusion, mistake or deception.” *Id.* § 1127.

⁶⁵ See, e.g., *Person’s Co. v. Christman*, 900 F.2d 1565, 1568–69 (Fed. Cir. 1990) (“The concept of territoriality is basic to trademark law; trademark rights exist in each country *solely* according to that country’s statutory scheme.”) (emphasis added) (footnote omitted).

⁶⁶ See Endeshaw, *supra* note 62, at 324 (explaining that marks normally can have legal effect only in the specific territory where they are registered, or, in cases of non-registered marks, where they established themselves). Some famous marks, however, are protected beyond strictly defined territory. See 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 29:4 (2003) [hereinafter MCCARTHY ON TRADEMARKS].

legal schemes giving effect to such marks.⁶⁷ Domain names, by contrast, are both unique and global in nature. Only one entity in the world can obtain the right to use a specific domain name, and that domain name that can be accessed globally.⁶⁸

2. The Prehistory of Cybersquatting Regulation

When mark owners started to realize the commercial power and value of incorporating their marks in domain names, it was sometimes too late. The domain name registration system was not interested in trademark rights and supplied registrations to whoever was willing to pay the appropriate fee on a “first come, first served” basis.⁶⁹ Some of the “early bird” registrants did not have any rights to the marks. When this led to wholesale registrations of domain names by registrants who held the domain names “for ransom,”⁷⁰ mark owners decided to fight back against these cybersquatting activities.⁷¹ Early on, the most effective tools in the U.S. legal system to combat cybersquatting were traditional trademark and unfair competition law and the relatively new

⁶⁷ The territoriality doctrine, however, under which a trademark is recognized as having a separate existence in each sovereign territory in which it is registered or legally recognized, has been criticized as “obsolete in a world market where information products like computer programs cannot be located at a particular spot on the globe.” MCCARTHY ON TRADEMARKS, *supra* note 66, § 29:1, at 29-4 to -6.

⁶⁸ Technically, it is more accurate to say that only one registrant may have exclusive rights in a certain SLD (such as <yahoo>) under a certain TLD (such as <.com>). *See, e.g.,* Frankel, *supra* note 9, at 870–72 (noting the uniqueness of a domain name and describing the significance of that uniqueness).

⁶⁹ *See* A. Michael Fromkin, *ICANN’s “Uniform Dispute Resolution Policy”—Causes and (Partial) Cures*, 67 BROOK. L. REV. 605, 620 (2002) (noting that “registration of SLDs in the three existing gTLDs (.com, .org, and .net) and in the ccTLDs which emulate them, is on a first-come, first-served basis”).

⁷⁰ One court described cybersquatting as “the registration as domain names of well-known trademarks by non-trademark holders who then try to sell the names back to the trademark owners . . . who not infrequently have been willing to pay ‘ransom’ in order to get ‘their names’ back.” *See* *Sporty’s Farm L.L.C. v. Sportsman’s Mkt., Inc.*, 202 F.3d 489, 493 (2d Cir. 2000) (citing H.R. REP. NO. 106-412, at 5–7 (1999) and S. REP. NO. 106-140, at 4–7 (1999)).

⁷¹ Generally, cybersquatting is referred to as the unlawful registration of domain names incorporating trademarks in which others have rights. One Senate report defined cybersquatting as “the deliberate, bad-faith, and abusive registration of Internet domain names in violation of the rights of trademark owners.” S. REP. NO. 106-140, at 4 (1999).

Federal Trademark Dilution Act (“FTDA”),⁷² the latter of which was incorporated into the U.S. Trademark Act of 1946 (“Lanham Act”).⁷³

Section 32(1) of the Lanham Act⁷⁴ protects registered mark owners against the use of their trademarks in cases of likelihood of confusion as to the source of the goods and services. This protection was sometimes hard to implement in cases of cybersquatting because many cybersquatters never tried to confuse consumers as to the source of any goods or services. Often, the cybersquatter never posted anything on the Web site because the intention was eventually to sell the domain name for profit to the mark holder.⁷⁵ Section 43(a) of the Lanham Act⁷⁶ protects mark owners—including non-registered marks—against false advertising and confusion as to the source, sponsorship, and affiliation of goods and services. In both cases, the hallmarks of trademark protection are in the concepts of “likelihood of confusion”⁷⁷ and “use in commerce.”⁷⁸

⁷² Federal Trademark Dilution Act of 1995, Pub. L. No. 104-98, 109 Stat. 985 (1996) (codified as amended at 15 U.S.C. § 1125(c) (2000)).

⁷³ 15 U.S.C. §§ 1051–1129 (2000).

⁷⁴ *Id.* § 1114(1).

⁷⁵ See J. Thomas McCarthy, *Trademarks, Cybersquatters and Domain Names*, 10 DEPAUL-LCA J. ART & ENT. L. & POL’Y 231, 245 (2000) (“The usual cybersquatter has no interest in using the domain name to identify a website. The cybersquatter typically wants only to warehouse the name and deprive the legitimate owner of its use, releasing it only for a fee.”).

⁷⁶ 15 U.S.C. § 1125(a).

⁷⁷ See, e.g., *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, 163–64 (1995) (stating that trademark law protects consumers from a likelihood of confusion as to the source of products, and also assures that mark owners will reap the financial benefits of products bearing their marks); Anahid Chalikian, Comment, *Cybersquatting*, 3 J. LEGAL ADVOC. & PRAC. 106, 107 (2001) (stating that the hallmark of any trademark infringement or false advertising claim is the likelihood of confusion).

⁷⁸ For example, 15 U.S.C. § 1051(a)(1) indicates that only trademarks “used in commerce” can register in the U.S. principal register. In an Intent to Use (“ITU”) application for registration in the principal registrar, the applicant must give a formal statement of his or her “bona fide intention to use the mark in commerce.” *Id.* § 1051(b)(3)(B). In addition, an ITU applicant must supply a “verified statement that the mark is in use in commerce” within six months after the date of the notice of allowance. *Id.* § 1051(d)(1). Use in commerce by the defendant is also a prerequisite for filing a civil action against unlawful competing use under 15 U.S.C. § 1125(a)(1).

Because of the complications in applying traditional trademark concepts to prevent cybersquatting, the more popular tool was the FTDA, which provides injunctive relief to owners of famous marks against dilution of the distinctive quality of the mark.⁷⁹ Dilution may occur either as a result of “blurring” or “tarnishment” of the famous mark.⁸⁰ The benefit for mark owners under the FTDA was that they did not have to prove likelihood of consumer confusion in dilution claims.⁸¹ Nevertheless, the use in commerce requirement remains intact.⁸²

In applying traditional trademark law tests or trademark dilution principles in cybersquatting cases, the first question is whether incorporation of the mark in a domain name constituted unlawful trademark infringement or dilution.⁸³ In analyzing this issue, courts tried to incorporate trademark and dilution concepts into domain name disputes, recognizing the dual purpose of

⁷⁹ *Id.* § 1125(c); see also Jason R. Edgecombe, Comment, *Off The Mark: Bringing the Federal Trademark Dilution Act in Line with Established Trademark Law*, 51 EMORY L.J. 1247 (2002) (providing an overview of the Federal Trademark Dilution Act (“FTDA”)).

⁸⁰ Edgecombe, *supra* note 79, at 1253–56 (describing these two traditional forms of dilution). The concept of cybersquatting causing dilution was applied in *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1239–41 (N.D. Ill. 1996).

⁸¹ See *supra* text accompanying notes 63–64. Indeed, one of the explicit goals of the FTDA was to help fight cybersquatters. As Senator Leahy of Vermont stated, “it is my hope that this antidilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others.” 141 CONG. REC. 38,561 (1995) (statement of Sen. Leahy).

⁸² The statute reads:

The owner of a famous mark shall be entitled . . . to an injunction against another person’s *commercial use in commerce* of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection.

15 U.S.C § 1125(c)(1) (emphasis added).

⁸³ Professor McCarthy, the trademark scholar, observes that “[t]he relationship between domain names and trademark law falls into two parts: validity and infringement.” McCarthy, *supra* note 75, at 241. The validity question is whether a domain name is, or can become, a trade or service mark, and McCarthy confidently answers in the affirmative. See *id.* at 241–42. As to whether a domain name can infringe someone else’s valid trademark or service mark, however, McCarthy finds the issue more complex. See *id.* at 242–43; see also Sharrock, *supra* note 17, at 840 n.131 (suggesting that TLDs such as <.com> or <.net> are not individually capable of serving as trademarks, since they are not capable of being source identifiers).

domain names in the contemporary world of commerce. As one commentator observed:

The domain name serves a dual purpose. It marks the location of the site within cyberspace, much like a postal address in the real world, but it may also indicate to users some information as to the content of the site, and, in instances of well-known trade names or trademarks, may provide information as to the origin of the contents of the site.⁸⁴

Courts have recognized that potential customers of well-known mark holders will be discouraged if they cannot find that company's mark at its most obvious location, "but instead are forced to wade through hundreds of web sites."⁸⁵ Addressing the problem in *Panavision International L.P. v. Toeppen*, the Ninth Circuit observed that "[a] significant purpose of the domain name is to identify the entity that owns the web site."⁸⁶ Affirming an FTDA ruling against a cybersquatting defendant, the court found the defendant's use of the plaintiff's mark in its domain name "diminished 'the capacity of the [plaintiff's] marks to identify and distinguish [its] goods and services on the Internet.'"⁸⁷

The second problem was the commercial use requirement. In *Avery Dennison Corp. v. Sumpton*, the Ninth Circuit held that the mere registration of a domain name is not, in and of itself, a "commercial use" for the purposes of dilution.⁸⁸ In the *Panavision* case, however, the cybersquatter only used the allegedly diluting domain name to post on his Web site views of the landscape of

⁸⁴ Peter Brown, *New Issues in Internet Litigation*, in 17TH ANNUAL INSTITUTE ON COMPUTER LAW: THE EVOLVING LAW OF THE INTERNET-COMMERCE, FREE SPEECH, SECURITY, OBSENY AND ENTERTAINMENT, at 151, 156 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 471, 1997), *quoted in* *Panavision Int'l L.P. v. Toeppen*, 141 F.3d 1316, 1327 n.8 (9th Cir. 1998).

⁸⁵ *Panavision*, 141 F.3d at 1327.

⁸⁶ *Id.*

⁸⁷ *Id.* at 1326 (quoting 945 F. Supp. 1296, 1304 (C.D. Cal. 1996) (district court opinion)). This kind of dilution developed by the court was sometimes called "dilution by elimination." See Ronald Abramson, *Internet Domain Litigation, 1999*, in ADVANCED SEMINAR ON TRADEMARK LAW, at 7, 20-21 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 558, 1999).

⁸⁸ 189 F.3d 868, 879-80 (9th Cir. 1999).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 47

Pana, Illinois, but the court nevertheless found a commercial use because the cybersquatter tried to profit by the resale of the domain name to the entity conducting business under it.⁸⁹ In other words, the court concluded that a cybersquatter might be subject to injunction under the FTDA even if its only business is to trade domain names with the corresponding mark owners for commercial gain.

U.S. courts have stretched trademark law, and especially the FTDA, “like a rubber band” to strike down cybersquatters.⁹⁰ Thus, even before the enactment of the ACPA, cybersquatters were, in many cases, successfully defeated in courts. Some problems remained unsolved, however, such as cybersquatting activities that did not fall within the protection against dilution by blurring or tarnishing a famous mark.⁹¹ In addition, the FTDA protects only famous marks; non-famous marks are left outside of its scope.⁹² At that time, it was clear that some troubling questions remained unsolved, for example when registrants sought to profit from the “non-mark” value of the domain name, such as in the case of surnames.⁹³ Finally, the problem of commercial use was not entirely solved by the case law. For example, existing law left a gap for sophisticated cybersquatters who did not show any attempt to sell the domain name to the mark owners, but also made no

⁸⁹ See *Panavision*, 141 F.3d at 1325 (quoting *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1230 (N.D. Ill. 1996)).

⁹⁰ McCarthy, *supra* note 75, at 247.

⁹¹ Even given the judicial activist approach that courts were willing to take against cybersquatters, it remained uncertain how much further courts should go while facing more and more sophisticated activities. See generally *id.* at 245–49.

⁹² At that time, some commentators expressed the concern that courts will artificially extend beyond recognition the concept and interpretation of “famousness” out of their desire to help mark owners in their war against cybersquatting. See, e.g., Michael B. Landau, *Problems Arising Out of the Use of “WWW.TRADEMARK.COM”: The Application of Principles of Trademark Law to Internet Domain Name Disputes*, 13 GA. ST. U. L. REV. 455, 478–80 (1997). One commentator suggested that the district court’s expansion of the commercial use requirement in *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227 (N.D. Ill. 1996), “went beyond even the most elastic interpretation of the class of goods that the mark will have been registered for . . . and the broadest allowance for the plausible boundary of the specific (famous) mark.” Endeshaw, *supra* note 62, at 337.

⁹³ See, e.g., *Avery Dennison Corp. v. Sumpton*, 189 F.3d 868, 879–81 (9th Cir. 1999) (indicating that the Ninth Circuit did not consider as typical cybersquatting the wholesale trade in domain names ending in <.net>, offered for sale for their non-trademark value).

other commercial use of it. Given the trouble and expenses involving long, expensive, and complex litigation against the cybersquatters, some mark owners simply preferred to pay off the ransom.⁹⁴ Professor J. Thomas McCarthy argued that even with the FTDA, “there was a poor fit between the actions of the typical cybersquatter and the federal trademark law as it existed” before the enactment of the ACPA.⁹⁵

II. THE NEW LEGAL FRAMEWORK

After reviewing the problematic juncture of trademarks and domain names, it is evident why change was imperative.⁹⁶ In late 1999, intense pressure from the trademark owner community led to the creation of two important mechanisms designed to address domain name disputes and thwart cybersquatting:⁹⁷ the Anticybersquatting Consumer Protection Act (“ACPA”) and the Uniform Dispute Resolution Policy (“UDRP”). This part provides an overview on these two important developments and notes some of the relevant court decisions interpreting them.

A. *The UDRP*

1. The UDRP Mechanism in Brief

The UDRP⁹⁸ is incorporated by reference into all ICANN-controlled registration agreements of generic top-level domains

⁹⁴ See, *Sporty's Farm L.L.C. v. Sportsman's Market, Inc.*, 202 F.3d 489, 493 (2d Cir. 2000) (indicating that the speculative registration of domain names “prevents use of the domain name by the mark owners, who not infrequently have been willing to pay ‘ransom’ in order to get ‘their names’ back” (citing H.R. REP. NO. 106-412, at 5–7 (1999); S. REP. NO. 106-140, at 4–7 (1999))).

⁹⁵ McCarthy, *supra* note 75, at 245.

⁹⁶ Congress decided that legislation was “needed to clarify the rights of trademark owners with respect to bad faith, abusive domain name registration practices, to provide clear deterrence to prevent bad faith and abusive conduct, and to provide adequate remedies for trademark owners in those cases where it does occur.” S. REP. NO. 106-140, at 7–8 (1999).

⁹⁷ See *supra* note 70 (defining cybersquatting).

⁹⁸ ICANN, UNIFORM DISPUTE RESOLUTION POLICY (1999), at <http://www.icann.org/dndr/udrp/policy.htm> (last visited Oct. 31, 2003) [hereinafter UDRP or POLICY].

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 49

such as <.com>, <.net>, and <.org>.⁹⁹ The UDRP controls the rights and obligations of the domain name registrant *vis-à-vis* the registrar in cases of a third party's claims regarding the registration.¹⁰⁰ The UDRP is sometimes called a mandatory or administrative arbitration mechanism, since it created a compulsory tribunal to adjudicate cybersquatting claims.¹⁰¹ What makes the UDRP so powerful and unavoidable is that, by virtue of an exclusive agreement with the U.S. Department of Commerce, ICANN is the only entity responsible for the administration of the domain name system.¹⁰² ICANN's contracts with the gTLD registries compel the incorporation of the UDRP in all contracts between these gTLD registries and commercial registrars, who, in turn, incorporate the UDRP in all registration agreements with gTLD registrants.¹⁰³ Hence, since 1999 all ICANN-controlled gTLD registrants must adhere to the UDRP.¹⁰⁴

⁹⁹ See Froomkin, *supra* note 69, at 716 (explaining that ICANN requires all registrants in gTLDs such as <.com> to agree to a mandatory online dispute resolution process).

¹⁰⁰ The Policy provides:

This Uniform Domain Name Dispute Resolution Policy . . . has been adopted by the Internet Corporation for Assigned Names and Numbers . . . is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you.

UDRP, *supra* note 98, ¶ 1.

¹⁰¹ A more accurate description of the UDRP, however, portrayed it as "a hybrid decision-making structure that draws on elements found in arbitration, adjudication, and ministerial decision-making systems." Laurence R. Helfer & Graeme B. Dinwoodie, *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*, 43 WM. & MARY L. REV. 141, 154 (2001).

¹⁰² See Michael Geist, *FAIR.COM?: An Examination of the Allegations of Systematic Unfairness in the ICANN UDRP*, 27 BROOK. J. INT'L L. 903, 913-21 (2002) (chronicling the developments leading to ICANN's creation and noting that "the U.S. government approved the creation of ICANN, granting the new non-profit corporation the responsibility for centralizing the management of the DNS").

¹⁰³ See Keith Blackman, *The Uniform Domain Name Dispute Resolution Policy: A Cheaper Way to Hijack Domain Names and Suppress Critics*, 15 HARV. J.L. & TECH. 211, 228 (2001) (noting that the UDRP and its accompanying rules are incorporated by reference into all registration agreements with approved registrars).

¹⁰⁴ For a timeline of the implementation of the Policy, see ICANN, *Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy*, at <http://www.icann.org/udrp/udrp-schedule.htm> (last visited Oct. 31, 2003).

The UDRP consists of a policy¹⁰⁵ as well as rules.¹⁰⁶ It was crafted to interfere only with blunt and straightforward cases of infringing registrations.¹⁰⁷ In such a typical case, the registrant, having no rights in a mark, takes advantage of the fact that domain names are assigned on a first come, first served basis and registers an attractive domain name—or often, many domain names—incorporating an established mark.¹⁰⁸ Under the UDRP, a complainant must prove three elements: (1) the domain name is identical or confusingly similar to a mark in which the complainant has rights; (2) the registrant has no legitimate interests in respect of the domain name; and (3) the domain name has been registered and is being used in bad faith.¹⁰⁹ Once these three elements are satisfied, the UDRP panel is entitled to order the cancellation of the domain name or its transfer to the complainant.¹¹⁰ The UDRP also supplies a non-exclusive list of circumstances indicating registration and use in bad faith,¹¹¹ and a non-exclusive list of

¹⁰⁵ See *supra* note 98.

¹⁰⁶ See ICANN, RULES FOR UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY (1999), at <http://www.icann.org/dndr/udrp/uniform-rules.htm> (last visited Oct. 31, 2003) [hereinafter UDRP RULES].

¹⁰⁷ See David E. Sorkin, *Judicial Review of ICANN Domain Name Disputes Decisions*, 18 SANTA CLARA COMPUTER & HIGH TECH. L.J. 35, 46 (2001) (noting that the UDRP, at least theoretically, is intended to cover only a narrow range of domain name disputes); Helfer & Dinwoodie, *supra* note 101, at 183–84 (describing the reaffirmation of a narrow-in-scope UDRP concept and citing relevant parts of ICANN’s Second Staff Report, which significantly shaped the Policy in its final version).

¹⁰⁸ See, e.g., *Panavision Int’l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998); *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227 (N.D. Ill. 1996).

¹⁰⁹ See UDRP, *supra* note 98, ¶ 4(a).

¹¹⁰ See *id.* ¶ 3.

¹¹¹ See *id.* ¶ 4(b). Under the UDRP, the following circumstances, “in particular but without limitation,” demonstrate the bad-faith registration and use of a domain name:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 51

affirmative defenses showing legitimate interests in the domain name.¹¹²

The UDRP has been a very popular tool for mark owners seeking recourse against possible cybersquatters.¹¹³ One of the major reasons for the UDRP's popularity among mark owners is its fast, streamlined, and effective process.¹¹⁴ Since the UDRP draws its power from the registration agreement that uniformly incorporates this mechanism, it is not limited by geographical boundaries. As noted, the UDRP was explicitly not meant to bind a court deciding on the same dispute. Before, after, and in the course of the UDRP process, registrants are entitled to commence a legal action in court,¹¹⁵ and the court's decision, once rendered, is

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

Id.

¹¹² *See id.* ¶ 4(c). Under the UDRP, the following circumstances, "in particular but without limitation," indicate rights and legitimate interests in a domain name:

- (i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or
- (ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or
- (iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

Id.

¹¹³ According to ICANN's Web site, as of September 10, 2003, more than 8,500 proceedings were filed to UDRP panels, concerning more than 14,500 domain names. *See* ICANN, *Summary of Status of Proceedings*, at <http://www.icann.org/udrp/-proceedings-stat.htm> (last updated Sept. 10, 2003).

¹¹⁴ *See, e.g.*, UDRP RULES, *supra* note 106, ¶ 5(a) (registrant must file a response to the complaint within 20 days of the "day of commencement"); *id.* ¶ 6 (a panel is generally appointed within five days of the filing of the response); *id.* ¶ 15(b) (decision should be rendered by the panel, absent of exceptional circumstances, within fourteen days of its appointment).

¹¹⁵ *See, e.g.*, *BroadBridge Media, L.L.C. v. Hypercd.com*, 106 F. Supp. 2d 505, 508–09 (S.D.N.Y. 2000) (concluding that a plaintiff that has filed an ICANN administrative proceeding may bring action in federal court before, during, and after filing the ICANN proceeding).

decisive with respect to the rights in the domain name.¹¹⁶ Additionally, if a losing registrant in the UDRP proceeding, whose domain name has been ordered cancelled or transferred, files a complaint in a court of mutual jurisdiction¹¹⁷ within ten business days from the panel's decision, execution of the panel's ruling has an automatic stay until the court decides on the matter or until the dispute is otherwise resolved.¹¹⁸

2. The Mutual Jurisdiction Problem and Rule 3(b)(xiii)

At this point, it is important to highlight an often-overlooked aspect of the UDRP rules. Rule 3(b)(xiii) provides that a trademark owner wishing to file a complaint against a registrant, must, as part of the procedural act of filing the complaint to the panel, submit to the jurisdiction of the courts in at least one specified "mutual jurisdiction."¹¹⁹ This provision is relevant in those cases where the mark owner wins the UDRP proceeding and the registrant subsequently wants to challenge the panel's decision in court.¹²⁰ Mutual jurisdiction is defined in the rules as:

[A] court jurisdiction at the location of either (a) the principal office of the Registrar . . . or (b) the domain-name holder's address as shown for the registration of the domain name in Registrar's Whois database at the time the complaint is submitted to the Provider.¹²¹

Reading this definition, it becomes apparent that the registrant has complete control over the determination of which court would be a mutual jurisdiction court.¹²² Obviously, the registrant can decide with which registrar to register the domain name and may make that choice based on which registrar has its principal office

¹¹⁶ See *id.*; see also UDRP, *supra* note 98, ¶ 4(k).

¹¹⁷ See *infra* Part II.A.2 (explaining the concept of mutual jurisdiction).

¹¹⁸ See UDRP, *supra* note 98, ¶ 4(k).

¹¹⁹ See UDRP RULES, *supra* note 106, ¶ 3(b)(xiii).

¹²⁰ See Helfer & Dinwoodie, *supra* note 101, at 186 (describing the process of approving the concept of mutual jurisdiction in the final version of the UDRP).

¹²¹ See UDRP RULES, *supra* note 106, ¶ 1; see also *infra* note 124 (defining a "Whois" directory). "Registrar" is defined in the rules as "the entity with which the Respondent [i.e., registrant] has registered a domain name that is the subject of a complaint." UDRP RULES, *supra* note 106, ¶ 1.

¹²² See Efroni, *supra* note 24, at 350 n.101.

in a preferred jurisdiction.¹²³ In addition, the registrant clearly decides which address to provide to the registrar, an address that ultimately appears in the registrar's Whois database.¹²⁴ Furthermore, a sophisticated registrant could merge the two options of mutual jurisdiction into one.¹²⁵ This aspect of the UDRP is important in cases when personal jurisdiction over the (potential) mark owner is questionable in a particular court, but the cybersquatter wants, nevertheless, to secure litigation in that favored jurisdiction.¹²⁶

B. The ACPA

The second mechanism controlling cybersquatting disputes is the ACPA.¹²⁷ Congress was convinced that the uncertainty as to the application of trademark law, inconsistent judicial decisions, and the growing phenomenon of cybersquatting needed to be remedied.¹²⁸ The result was the ACPA, a statute enacted in 1999¹²⁹ and incorporated into the Lanham Act. The ACPA includes two types of actions affording mark owners recourse in cybersquatting cases: in personam actions¹³⁰ and in rem actions.¹³¹

¹²³ Today, there are more than 170 registrars worldwide accredited by ICANN to sell domain names to consumers. See ICANN, *ICANN-Accredited Registrars*, at <http://www.icann.org/registrar/accredited-list.html> (last updated Oct. 28, 2003).

¹²⁴ A "Whois" directory is the list of registrants and their details run by the registration authority. See *Cable News Networks v. CNNews.com*, 177 F. Supp. 2d 506, 514 n.14 (E.D. Va. 2001) [hereinafter *CNN II*], *vacated in part on other grounds by CNN Appeal*, No. 02-1112, 2003 WL 152846; see also Network Solutions, *Whois Search*, at http://www.networksolutions.com/en_US/whois/index.jhtml (last visited Oct. 31, 2003).

¹²⁵ For example, a hypothetical registrant may wish to register a <.com> domain name and also make sure that in case he or she loses in the UDRP, any subsequent litigation regarding this registration shall take place in the state of Virginia. All that the registrant needs to do is to choose a Virginia-based registrar and supply to that registrar a Virginia address to appear in the Whois database.

¹²⁶ See discussion *infra* Part IV.C.1 (discussing possible litigation strategies of registrants).

¹²⁷ 15 U.S.C. §§ 1114, 1116, 1117, 1125, 1129 (2000).

¹²⁸ See *Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc.*, 202 F.3d 489, 495-96 (2d Cir. 2000) (citing H.R. REP. NO. 106-412, at 6 (1999) and S. REP. NO. 106-140, at 7 (1999)).

¹²⁹ See Anticybersquatting Consumer Protection Act of the Intellectual Property and Communications Omnibus Reform Act of 1999, Pub. L. No. 106-113, 113 Stat. 1501 (1999).

¹³⁰ See 15 U.S.C. § 1125(d)(1).

¹³¹ See *id.* § 1125(d)(2).

Another important section is the reverse domain name hijacking (“RDNH”) provision, designed to grant protection to registrants against unjustified cybersquatting claims.¹³²

1. In Personam Action

In an in personam action under the ACPA, the mark owner must first be able to establish in personam jurisdiction over the registrant.¹³³ The ACPA test for unlawful cybersquatting is three-prong. Registration of a domain name violates the ACPA if: (i) there is a protected mark involved, (ii) which, without regard to goods and services, a corresponding domain name was registered, trafficked or used, (iii) with a bad faith intent to profit from that activity.¹³⁴ One of the most important innovations of the ACPA is the substitution of the traditional use in commerce and likelihood of confusion or dilution elements with the “identical or confusingly similar” and “bad faith intent to profit” principles.¹³⁵ Courts generally reduce ACPA in personam analysis to three elementary questions: (1) whether the mark in question is distinctive or famous and therefore entitlement to protection under U.S. trademark law;¹³⁶ (2) whether the domain name is identical or confusingly similar to the mark;¹³⁷ and (3) whether there was a bad faith intent to profit on the part of the registrant.¹³⁸ Upon such finding, liability under the ACPA is generally imposed and the mark owner may win effective and powerful relief against the registrant, including forfeiture, cancellation, and transfer of the mark.¹³⁹ The ACPA also allows mark owners to seek statutory damages up to

¹³² See *id.* § 1114(2)(D)(v).

¹³³ See discussion *supra* Part I.B.1 (describing U.S. personal jurisdiction principles).

¹³⁴ See 15 U.S.C. § 1125(d)(1)(A).

¹³⁵ See *id.* Liability is imposed when “bad faith intent to profit” is established in registering, trafficking, or using a domain name that is identical with or confusingly similar to a distinctive mark, or identical, or confusingly similar to, or dilutive of a famous mark. See *id.* The provision makes no mention of a requirement of “use in commerce” or a “likelihood of confusion.” See *id.*

¹³⁶ See *id.* § 1125(a) (infringement); *id.* § 1125(c) (dilution).

¹³⁷ In the case of famous marks, the ACPA also protects against registrations that are dilutive of the mark, so long as the mark was famous at the time of the domain name’s registration. See *id.* § 1125(d)(1)(A)(ii)(II).

¹³⁸ See *Shields v. Zuccarini*, 254 F.3d 476, 482 (3d Cir. 2001).

¹³⁹ See 15 U.S.C. § 1125(d)(1)(C).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 55

\$100,000 per infringing domain name,¹⁴⁰ along with other Lanham Act remedies such as actual damages and attorneys' fees.¹⁴¹

2. In Rem Action

The drafters of the ACPA added the in rem provision to the new legislation, acknowledging that the speculative nature of cybersquatting activities may sometimes leave mark owners without an adequate in personam remedy.¹⁴² In order to apply in rem jurisdiction principles in domain name disputes, courts generally followed the legislative determination that domain names were property, or res, entitled to in rem jurisdiction,¹⁴³ with a "physical" location where the registration authorities are located.¹⁴⁴

¹⁴⁰ See *id.* § 1117(d).

¹⁴¹ See *id.* § 1117(a).

¹⁴² See H.R. CONF. REP. NO. 106-464, at 113-14 (1999) (explaining that the in rem provision is designed to lessen the difficulty faced by trademark owners when cybersquatters "register domain names under aliases or otherwise provide false information in their registration applications in order to avoid identification and service of process by the mark owner"); see also *Mattel, Inc. v. Barbie-Club.com*, 310 F.3d 293, 298 (2d Cir. 2002) (noting that the in rem provision "was provided in part to address the situation in which "a non-U.S. resident cybersquats on a domain name that infringes upon a U.S. trademark" (quoting 145 CONG. REC. H10823, H10826 (daily ed. Oct. 26, 1999))).

¹⁴³ See *Mattel*, 310 F.3d at 300 n.7 (noting that "Congress clearly intended to treat domain names as property for purposes of the ACPA's *in rem* provisions" (citing 145 CONG. REC. H10826 (daily ed. Oct. 26, 1999))); *Porsche Cars N. Am., Inc., v. Porsche.Net*, 302 F.3d 248, 260 (4th Cir. 2002) ("Congress may treat a domain name registration as property subject to in rem jurisdiction if it chooses, without violating the Constitution."); *Caesars World, Inc. v. Caesars-Palace.com*, 112 F. Supp. 2d 502, 504 (E.D. Va. 2000) ("There is no prohibition on a legislative body making something property. Even if a domain name is no more than data, Congress can make data property and assign its place of registration as its situs.").

¹⁴⁴ See *Mattel*, 310 F.3d at 301. The court stated:

[B]oth the language of the statute and its legislative history indicate that *in rem* jurisdiction is a preexisting fact determined by the location of the disputed domain name's registrar or a similar authority, and that the subsequent deposit of sufficient documents with a court of appropriate jurisdiction confirms the domain name's legal situs as being in that judicial district for purposes of the litigation.

Id. The court further found that the law's legislative history "makes it clear that Congress considered the 'registry or registrar' to provide a 'nexus' for *in rem* jurisdiction under the ACPA." *Id.* at 302 (quotation marks altered) (citing H.R. REP. NO. 106-412, at 14 (1999)); see also *Fleetboston Fin. Corp. v. Fleetbostonfinancial.com*, 138 F. Supp. 2d 121, 126 (D. Mass. 2001) (concluding that "the language of the ACPA restricts in rem

The language of the ACPA allows an in rem action when an in personam action is not feasible,¹⁴⁵ or when the registrant cannot be found through due diligence.¹⁴⁶ When the prerequisites for an in rem action are satisfied, “[t]he owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located.”¹⁴⁷ Remedies, however, under the in rem provision are limited to “a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.”¹⁴⁸

The in rem provision has recently been subject to intensive litigation. U.S. federal courts interpreting the in rem provision have reached several significant holdings:

- The proper judicial situs for filing an in rem action is the district in which the domain name registration authority resides, as opposed to any other U.S. jurisdiction.¹⁴⁹
- When both the registrant and registrar are foreign but the domain name registry is located in the United States, an in rem action in the district where the registry resides satisfies constitutional due process and the establishment of minimum contacts with that jurisdiction is not required.¹⁵⁰

jurisdiction to the judicial district in which the registrar, registry, or other domain name authority is located”).

¹⁴⁵ See 15 U.S.C. § 1125(d)(2)(A)(ii)(I) (2000); see also *Alitalia-Linee Aeree Italiane S.p.A. v. Casinoalitalia.Com*, 128 F. Supp. 2d 340, 344–45 (E.D. Va. 2001) (finding that the ACPA in personam and in rem provisions are mutually exclusive).

¹⁴⁶ See 15 U.S.C. § 1125(d)(2)(A)(ii)(II).

¹⁴⁷ See *id.* § 1125(d)(2)(A).

¹⁴⁸ See *id.* § 1125(d)(2)(D)(i).

¹⁴⁹ See *Fleetboston*, 138 F. Supp. 2d at 134 (concluding that allowing an aggrieved plaintiff to sue in the state of his or her choosing “would permit a procedure that plainly offends traditional notions of fair play and justice”).

¹⁵⁰ See *Porsche Cars N. Am., Inc., v. Porsche.Net*, 302 F.3d 248, 259–260 (4th Cir. 2002) (holding that in a case that directly concerns possession of the defendant domain names, the registrant’s other personal contacts with the forum are constitutionally irrelevant to the assertion of in rem jurisdiction over those domain names); see also *CNN I*, 162 F. Supp. 2d 484, 491 (E.D. Va. 2001) (“[I]n an ACPA *in rem* action, it is not necessary that the allegedly infringing registrant have minimum contacts with the forum;

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 57

- In order to succeed in an in rem action, proving registrant's bad faith is not required.¹⁵¹
- A federal injunction against a registry located in the United States is the proper means to enforce the federal court's decision to disable or cancel domain name registration,¹⁵² as well as transfer the registration to plaintiff.¹⁵³

3. The Reverse Domain Name Hijacking Provision

As previously noted,¹⁵⁴ the RDNH provision aims to protect registrants against unjustified cybersquatting claims. The provision states that a domain name registrant whose domain name has been suspended, disabled, or transferred under a reasonable policy may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful.¹⁵⁵ A court can then grant injunctive relief to the registrant, including the reactivation of the domain name or transfer of the domain name to the original registrant.¹⁵⁶

it is enough, as here, that the registry is located in the forum; it is enough, as here, that the registry is located in the forum.”).

¹⁵¹ See *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214, 227–32 (4th Cir. 2002).

¹⁵² See *GlobalSantaFe Corp. v. GlobalSantaFe.com*, 250 F. Supp. 2d 610, 623 (E.D. Va. 2003) (“[A] court is not limited merely to the disabling procedure envisioned by [the registry’s] contractual agreements, but may also order the registry to delete completely a domain name registration pursuant to the court’s order.”).

¹⁵³ See *Am. Online, Inc. v. AOL.org*, 259 F. Supp. 2d 449, 453–54 (E.D. Va. 2003).

¹⁵⁴ See *supra* text accompanying note 132. The Fourth Circuit’s *Barcelona.com* opinion ably explained the term “reverse domain name hijacking.” The court explained:

If a domain-name registrant cybersquats in violation of the ACPA, he “hijacks” the domain name from a trademark owner who ordinarily would be expected to have the right to use the domain name involving his trademark. But when a trademark owner overreaches in exercising rights under the ACPA, he “reverse hijacks” the domain name from the domain-name registrant. Thus, § 1114(2)(D)(v), enacted to protect domain-name registrants against overreaching trademark owners, may be referred to as the “reverse domain name hijacking” provision.

Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona, 330 F.3d 617, 625 n.1 (4th Cir. 2003).

¹⁵⁵ 15 U.S.C. § 1114(2)(D)(v).

¹⁵⁶ *Id.*

The provision is well illustrated by the First Circuit's opinion in *Sallen v. Corinthians Licenciamentos LTDA*.¹⁵⁷ David Sallen, a U.S. resident,¹⁵⁸ registered the domain name <www.corinthians.com> with Network Solutions Inc. ("NSI").¹⁵⁹ The famous Brazilian soccer team, Corinthians (Portuguese for "Corinthians"), which had, *inter alia*, Brazilian trademark rights in the mark CORINTHIAO, filed and won a complaint under the UDRP.¹⁶⁰ Within the required ten days, Sallen filed a federal lawsuit in the United States,¹⁶¹ seeking a declaratory judgment that his registration for the domain name did not violate the ACPA.¹⁶²

At some point, apparently for the purpose of intercepting the motion for declaratory judgment, the defendant soccer team disclaimed any intention to bring further ACPA claims against Sallen.¹⁶³ The defendant moved to dismiss Sallen's complaint, arguing that the district court lacked subject matter jurisdiction,¹⁶⁴ because Sallen requested a declaration of his rights under the ACPA and defendant had no intent to sue Sallen under the act.¹⁶⁵ Accepting defendant's argument, the district court ruled that there was no real controversy between the parties and thus, a declaratory judgment could not be obtained for lack of subject matter jurisdiction.¹⁶⁶ This interpretation suggests that under certain

¹⁵⁷ 273 F.3d 14 (1st Cir. 2001).

¹⁵⁸ *Id.* at 16.

¹⁵⁹ *Id.* at 20. At the time of registration in August 1998, Network Solutions Inc. ("NSI") was the only registry and registrar for domain names listed in the <.com> gTLD file. See *Barcelona.com*, 189 F. Supp. 2d 367, 370 (E.D. Va. 2002), *rev'd and vacated*, 330 F.3d 617 (4th Cir. 2003).

¹⁶⁰ See *Corinthians Licenciamentos LTDA v. David Sallen*, WIPO Case No. D2000-0461 (July 17, 2000), available at <http://arbitrator.wipo.int/domains/decisions/html/2000/d2000-0461.html> (last visited Nov. 3, 2003).

¹⁶¹ See *Sallen v. Corinthians Licenciamentos LTDA*, No. 00-CV-11555, 2000 U.S. Dist. LEXIS 19976 (D. Mass. Dec. 19, 2000).

¹⁶² See *Sallen*, 273 F.3d at 22.

¹⁶³ See *Sallen*, 2000 U.S. Dist. LEXIS 19976, at *1.

¹⁶⁴ See FED. R. CIV. P. 12(b)(1).

¹⁶⁵ See *Sallen*, 273 F.3d at 22. Interestingly, there is no indication in the *Sallen* district court's opinion that defendants moved to dismiss also for a lack of personal jurisdiction, and thus, this matter was not discussed. See *Sallen*, 2000 U.S. Dist. LEXIS 19976.

¹⁶⁶ The district court stated:

Based on the representations made by Defendant . . . that it "has no intent to sue Plaintiff under the ACPA for his past activities in connection with corinthians.com" the Motion to Dismiss is GRANTED . . . Jurisdiction under

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 59

circumstances, the UDRP decisions are indeed binding in the United States, despite the explicit intention of the policy's drafters and the language of the policy itself.¹⁶⁷

As a result of the district court's decision the domain name was transferred, and Sallen appealed to the First Circuit.¹⁶⁸ The appellate court reversed the district court's decision, holding that 15 U.S.C. § 1114(2)(D)(v) granted domain registrants who have lost domain names under UDRP administrative panel decisions an affirmative cause of action in federal court for a declaration of nonviolation of the ACPA and for the return of the wrongfully transferred domain names.¹⁶⁹ The court concluded:

Although [defendant] has stated that it has no intent to sue Sallen under the ACPA for his past actions related to corinthians.com, there is indeed a controversy between Sallen and [Corinthians Licenciamentos LTDA ("CL")]: Sallen asserts that he has rights to corinthians.com and CL asserts that it has mutually exclusive rights to the same domain name. Since the dismissal of Sallen's complaint, the corinthians.com domain name has been transferred to CL and is now being used to promote the Corinthians soccer team. Sallen asserts that the domain name belongs to him.¹⁷⁰

The court's decision rejected the defendants' argument that there was no case or controversy.¹⁷¹ Interestingly, at the time when the appellate decision was rendered, the motion for declaratory judgment was no longer appropriate since the domain name was no longer in Sallen's possession. The appellate court, however, offered a potential solution for future litigation, suggesting in a footnote that if Sallen had been given the

28 U.S.C. § 2201 [authorizing declaratory judgments] is proper only if there exists an actual controversy [sic] between the parties. Absent the threat of suit there is no controversy and jurisdiction is lacking.

Sallen, 2000 U.S. Dist. LEXIS 19976, at *1-2 (citation omitted).

¹⁶⁷ See *supra* text accompanying notes 115-118.

¹⁶⁸ *Sallen*, 273 F.3d at 25.

¹⁶⁹ See *id.* at 24-30.

¹⁷⁰ *Id.* at 25.

¹⁷¹ See *id.* at 25-30.

opportunity to amend his complaint, then he could have properly sought an injunction.¹⁷² This determination was the first indication from an appellate court that injunctions and declaratory relief under the RDNH provision are appropriate remedies for registrants seeking reversal of UDRP decisions.

Part of the controversy in *Sallen* involved language in the RDNH provision requiring notice to be given to the “mark owner” upon the filing of an action to establish that the use of a mark is not unlawful.¹⁷³ The defendant argued that the term “mark owner” in that statute refers only to registered U.S. trademarks.¹⁷⁴ Accordingly, the defendant argued that registrant protection under the RDNH provision cannot apply to its mark, which was registered in Brazil but not in the United States.¹⁷⁵ The *Sallen* court rejected this argument based on legal analysis of the language and definitions of the law.¹⁷⁶ In addition, the court provided a policy argument for broad reading of the provision:

[I]nterpreting “mark owner” to apply only to registered U.S. marks would create a perverse result at odds with our view of the ACPA as granting relief to registrants who have wrongly lost domain names in UDRP proceedings. It would be very odd if Congress, which was well aware of the international nature of trademark disputes, protected Americans against reverse domain name hijacking only when a registered American mark owner was doing the hijacking. Such a policy would permit American citizens,

¹⁷² See *id.* at 16 n.1. The court stated:

Sallen’s initiation of these proceedings in the district court stayed the WIPO panel’s order to transfer the domain name to [the defendant]. After the district court dismissed Sallen’s suit, however, the domain name was transferred to [Corinthians Licenciamentos LTDA], possibly wrongfully in light of a pending appeal. If the complaint were reinstated, the logic of Sallen’s position is that he would seek leave to amend his complaint to request an injunction returning the domain name.

Id. (citation omitted).

¹⁷³ See 15 U.S.C. § 1114(2)(D)(v) (A losing registrant “may, upon notice to the *mark owner*, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this chapter.”).

¹⁷⁴ *Sallen*, 273 F.3d at 24.

¹⁷⁵ *Id.* at 24 & n.10.

¹⁷⁶ *Id.* at 23–24.

whose domain names are subject to WIPO transfer orders, to get relief against abusive mark owners that have registered in the U.S., but not against abusive mark owners that have not registered (including both foreign mark owners and domestic mark owners that have not registered). *It would leave registrants unprotected against reverse domain name hijackers so long as the hijackers are not registered with the PTO.*¹⁷⁷

The court was obviously concerned that a narrow reading of the provision could yield absurd results, with registrants having no recourse against unregistered- or foreign-mark owners who have prevailed in a UDRP proceeding.¹⁷⁸ Another related jurisdictional question—one left unresolved even after *Sallen*—is whether an RDNH action requires establishment of in personam jurisdiction. This issue was not discussed in either the district court opinion or circuit court opinion in *Sallen*, and there is no indication in either opinion that the defendant, a foreign soccer team asserting a foreign trademark, introduced an in personam jurisdiction objection.¹⁷⁹ Because personal jurisdiction was not directly discussed in *Sallen*, the opinion leaves open an interesting question: could the U.S. registrant use in rem principles as an alternative jurisdictional basis for his or her RDNH claim?

As noted above, the ACPA in rem provision is not helpful when the mark is not protected in the United States.¹⁸⁰ In addition, the provision is available only to “the owner of a mark,” as distinguished from a domain name registrant.¹⁸¹ Lastly, the RDNH provision does not specifically provide for in rem jurisdiction. Thus, a court might conclude that absent personal jurisdiction over the defendant, the RDNH action should be dismissed.

The above quoted language from *Sallen*, however, provides a rationale for a different analysis leading to the opposite result. The *Sallen* court gave an expansive interpretation to the term “mark

¹⁷⁷ *Id.* at 24 (emphasis added) (footnote omitted).

¹⁷⁸ *Id.* at 23–24.

¹⁷⁹ See *Sallen v. Corinthians Licenciamentos LTDA*, No. 00-CV-11555, 2000 U.S. Dist. LEXIS 19976, at *1–*2 (D. Mass. Dec. 19, 2000); *Sallen*, 273 F.3d at 20–30.

¹⁸⁰ See 15 U.S.C. § 1125(d)(2)(A)(i) (2000) (protecting only Lanham Act marks).

¹⁸¹ See *id.*

owner” appearing in the RDNH provision. As explained by the court, the reason was to protect U.S. registrants, such as Sallen, against reverse-domain-name-hijacking commenced by foreign owners.¹⁸² Further requirement of personal jurisdiction over the defendant could easily frustrate the purpose of *Sallen*’s mark owner interpretation.¹⁸³

The comparison of *Sallen*’s mark owner interpretation to the rationale behind the legislation of the in rem provision is inevitable. It should not be hard to demonstrate how U.S. plaintiff-registrants might face difficult procedural setbacks in circumstances where foreign defendant-owners’ activity does not meet personal jurisdiction tests. Despite the fact that a winning UDRP mark owner may prevent a U.S. registrant from using a domain name worldwide and also in the United States—that is, over the Internet—the registrant would not be able to sue under the ACPA without establishing personal jurisdiction. This was exactly the problem that American mark owners faced while attempting to challenge foreign registrants under pre-ACPA American law, and this was exactly the reason why the in rem provision was legislated.¹⁸⁴

Put differently, *Sallen*’s “mark owner” interpretation coupled with ACPA in rem rationale may enable a court to *read* the in rem jurisdiction authority into the RDNH provision.¹⁸⁵ Although this is

¹⁸² *Sallen*, 273 F.3d at 24.

¹⁸³ In order to illustrate this point, assume that the defendant in the *Sallen* case had succeeded in a hypothetical personal jurisdiction objection. In such case, no matter how broad the term “mark owner” is interpreted, the court probably would have had to dismiss the suit due to lack of jurisdictional basis.

¹⁸⁴ See discussion *supra* Part II.B.2 (providing background to the legislation of the in rem provision).

¹⁸⁵ A pre-ACPA case suggested that the district court did not have jurisdiction in a suit filed against the domain names themselves absent specific authority provided in the relevant statutory language (in that case, by the FTDA) giving the court subject-matter jurisdiction. See *Porsche Cars N. Am., Inc. v. Porsch.com*, 51 F. Supp. 2d 707, 711–13 (E.D. Va. 1999), *vacated due to a superseding statute* by *Porsche Cars N. Am., Inc. v. Allporsche.com*, 215 F.3d 1320 (4th Cir. 2000) (table), and *remanded in part* by *Porsche Cars N. Am., Inc. v. Porsche.net*, 302 F.3d 248 (4th Cir. 2002). The court applied rule 4(n) of the Federal Rules of Civil Procedure to the FTDA and found that such in rem jurisdiction could not be exercised. *Id.* at 711–12. Without conducting a detailed comparison between the *Porsche* decision and a hypothetical application of in rem jurisdiction in a reverse domain name hijacking (“RDNH”) case, at least one commentary

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 63

purely a theoretical solution to a theoretical problem, it may draw attention to the fact that by using existing legal tools, U.S. courts might further extend the application of the ACPA also against foreign owners without the need to meet the burden of personal jurisdiction and perhaps, where such owner has no minimum contacts with the United States.¹⁸⁶

Despite this area of uncertainty, the *Sallen* decision represents an important moment in U.S. domain name disputes jurisprudence. It provides that a losing registrant may bring a RDNH action against the mark owner and obtain relief before and after the implementation of the UDRP. Further, the opinion illustrates a crucial point: under the ACPA, registrants should be able to attack UDRP decisions in disputes involving *any kind of marks*, U.S. and foreign. As will be discussed further, this aspect of *Sallen* bears important consequences for international domain name disputes litigated in the United States.

III. THE *BARCELONA.COM* DISPUTE

After this long but necessary background, this Article turns its focus to the Fourth Circuit's June 2003 opinion in the case of *Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona*,¹⁸⁷ which unanimously reversed, vacated, and remanded the lower court's decision, rendered by Chief Judge Claude M. Hilton of the District Court for the Eastern District of Virginia.¹⁸⁸

has suggested that application of in rem jurisdiction does not require specific authority in the law. See Thomas R. Lee, *In Rem Jurisdiction in Cyberspace*, 75 WASH. L. REV. 97, 117 (2000). Professor Lee stated:

The *Porsche Cars* court's analysis misconstrues the very nature of in rem jurisdiction. A proceeding *in rem* is not an anomalous action requiring special statutory authorization to overcome some sort of disfavored status. Rather, the designation "*in rem*" is one of two longstanding bases on which a court traditionally has acquired territorial jurisdiction over a dispute.

Id.

¹⁸⁶ As described *infra* Part IV.D.1, it appears that U.S. courts do not require the establishment of minimum contacts over foreign registrants in ACPA in rem provision actions.

¹⁸⁷ 330 F.3d 617 (4th Cir. 2003).

¹⁸⁸ *Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona*, 189 F. Supp. 2d 367 (E.D. Va. 2002), *rev'd and vacated*, 330 F.3d 617 (4th Cir. 2003).

Section A of this part describes the factual background of the dispute over the domain name <www.barcelona.com> between a Spanish couple and the City Council of Barcelona, Spain. Subsection B describes the Fourth Circuit's decision on appeal.

A. *The Facts*¹⁸⁹

In February 1996, Joan Nogueras Cobo ("Nogueras"), a Spanish citizen, registered the domain name <www.barcelona.com> in the name of his wife with the U.S. registrar, NSI.¹⁹⁰ On the Web site, the couple provided tourist information about Barcelona, e-mail services, a chat room, and links to other Web sites.¹⁹¹ In early 1999, the Nogueras e-mailed the mayor of Barcelona ("Mayor") through a Web form on the official Web site of the City Council of Barcelona ("City Council"), proposing to negotiate with the City Council for its acquisition of the Web site, but Nogueras received no response.¹⁹²

Later that year, Nogueras and a business partner formed Barcelona.com, Inc. under Delaware law to own and run the Web site.¹⁹³ Although the Barcelona.com, Inc. maintains a New York mailing address, it has no employees in the United States, does not own or lease office space in the country, and does not have a phone listing in the United States.¹⁹⁴ Furthermore, its computer server is in Spain.¹⁹⁵

In March 2000, the City Council contacted Nogueras to learn more about the corporation and its plans for the domain name. Nogueras and his marketing director met with City Council representatives and later sent them a business plan for the Web site.¹⁹⁶ The negotiations did not ripen into an agreement, however,

¹⁸⁹ In describing the background of the dispute, the relies on the facts as described in both the district court and circuit court decisions.

¹⁹⁰ *Barcelona.com*, 189 F. Supp. 2d at 369.

¹⁹¹ *Id.*

¹⁹² *Barcelona.com*, 330 F.3d at 620.

¹⁹³ *Id.*

¹⁹⁴ *Id.*

¹⁹⁵ *Id.*

¹⁹⁶ *Id.* Soon after the city council made its demand, Norgueras had the domain name transferred from his wife's name to the corporation, which he had neglected to do in 1999 when the corporation was formed. *Id.* at 620–21.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 65

and in May 2000 the City Council demanded the transfer of the domain name to its possession.¹⁹⁷

After Barcelona.com, Inc. refused to surrender the domain name, the City Council, which owned numerous trademark registrations in Spain incorporating the word Barcelona,¹⁹⁸ launched a UDRP proceeding against the registrants claiming that the registration of the domain name violated the UDRP.¹⁹⁹ The City Council won the UDRP proceeding, with a panelist²⁰⁰ from the World Intellectual Property Organization (WIPO) concluding, *inter alia*, (1) that the city had trademark rights in the term Barcelona under Spanish law, and (2) that the domain name was registered and used in bad faith.²⁰¹ Thus, the registration was held to violate the UDRP.²⁰² Consequently, the domain name was ordered transferred to the City Council, in accord with the UDRP authority.²⁰³ Before the execution of the transfer order, Barcelona.com, Inc. commenced a lawsuit in the District Court for the Eastern District of Virginia, seeking declaratory judgment and asserting, *inter alia*, that the registration of the domain name was not unlawful.²⁰⁴ Consequently, and in accordance with the UDRP rules, the transfer was automatically halted until a further ruling by the district court.²⁰⁵

The district court's decision validated the transfer, concluding that under Spanish law the City Council was probably the rightful owner of all marks incorporating the term Barcelona.²⁰⁶ Furthermore, the district court concluded that the registrants demonstrated "bad faith intent to profit" and therefore, the

¹⁹⁷ *Id.* at 621.

¹⁹⁸ *Id.*

¹⁹⁹ See *Excelentísimo Ayuntamiento de Barcelona v. Barcelona.com, Inc.*, WIPO Case No. D2000-0505 (Aug. 4, 2000), available at <http://arbiter.wipo.int/domains/-decisions/html/2000/d2000-0505.html> (last visited Nov. 3, 2003).

²⁰⁰ In this instance, a single WIPO panelist, Marino Porzio, rendered the UDRP decision. *Id.*

²⁰¹ *Id.* ¶ 5.

²⁰² *Id.*

²⁰³ *Id.* ¶ 6.

²⁰⁴ *Barcelona.com*, 189 F. Supp. 2d at 369.

²⁰⁵ See UDRP, *supra* note 98, ¶ 4(k).

²⁰⁶ *Barcelona.com*, 189 F. Supp. 2d at 372.

registration could not be declared “not unlawful.”²⁰⁷ The district court also discussed the City Council cybersquatting counterclaims and found that the ACPA also protected foreign marks against cybersquatting.²⁰⁸ Since the City Council demonstrated that it had valid rights under the law of Spain, and since the domain name was identical or confusingly similar to the marks owned by the city, the prayer for a declaratory judgment in favor of the registrants was denied.²⁰⁹

B. *The Forth Circuit Ruling*

The Fourth Circuit in a unanimous opinion reversed, vacated, and remanded the lower court’s decision to validate the transfer of the mark to the City Council.²¹⁰ The Forth Circuit’s analysis, as laid out in its opinion, has four key aspects: (1) jurisdictional issues; (2) applicability of foreign law; (3) elements of the RDNH provision; and (4) the protection extended under U.S. law to the Barcelona mark.²¹¹

1. Jurisdictional Issues

First, the court determined that under the ACPA’s RDNH provision,²¹² it had subject matter jurisdiction,²¹³ in accord with the First Circuit’s decision in the case of *Sallen v. Corinthians Licenciamentos LTDA*.²¹⁴ As noted earlier in this Article, the RDNH provision confers a specific cause of action and relevant remedies in a federal court to a registrant losing in a UDRP proceeding and seeking to reverse the panel’s decision and retain his or her domain name registration.²¹⁵ The provision, in essence, gives the losing registrant a second chance to prove in federal court

²⁰⁷ *Id.* at 372–73.

²⁰⁸ *Id.* at 373–76. *See also infra* note 262 (discussing these “counterclaims” that apparently were never filed).

²⁰⁹ *See id.* at 376–77.

²¹⁰ *Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona*, 330 F.3d 617 (4th Cir. 2003).

²¹¹ *See id.*

²¹² 15 U.S.C. § 1114(2)(D)(v) (2000).

²¹³ *Barcelona.com*, 330 F.3d at 623.

²¹⁴ 273 F.3d 14 (1st Cir. 2001).

²¹⁵ *See supra* Part II.B.3.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 67

that the registration is not unlawful under the Lanham Act. Tracing back to the policy behind the ACPA and the objectives of Congress in enacting it, the court concluded that “because the UDRP is susceptible of being grounded on principles foreign or hostile to American law, the ACPA authorizes reversing a panel decision if such a result is called for by application of the Lanham Act.”²¹⁶

The general rule allowing the registrant’s cause of action was already determined in *Sallen*.²¹⁷ In this case, *Barcelona.com, Inc.* was a domain name registrant that lost its registration in a UDRP proceeding, and hence, the ACPA gave the court subject matter jurisdiction over the dispute.²¹⁸ The City Council argued that upon filing the complaint to the UDRP panel it agreed to be subject to the jurisdiction of “the Courts of Virginia (United States), only with respect to any challenge that may be made by [Nogueras] to a decision by the Administrative Panel to transfer or cancel the domain name that are subject to this complaint.”²¹⁹ In line with this argument, the City Council, as understood by the court, agreed to submit to the jurisdiction of the federal court in a suit under the RDNH provision. According to the City Council’s theory, however, the federal court was limited to the law applied in the panel’s decision—in this case, Spanish trademark law.²²⁰ Put differently, the City Council partially objected to the jurisdiction of the federal court, at least with respect to the potential application of U.S. law.

The court, rejecting this contention, reiterated that the UDRP proceeding is not jurisdictional in nature.²²¹ At the end of part II of

²¹⁶ *Barcelona.com*, 330 F.3d at 626.

²¹⁷ See *Sallen*, 273 F.3d at 28 (explaining that “a federal court’s interpretation of the ACPA supplants a WIPO panel’s interpretation of the UDRP”), noted in *Barcelona.com*, 330 F.3d at 626.

²¹⁸ *Barcelona.com*, 330 F.3d at 623.

²¹⁹ *Id.* at 621 (citing the City Council’s complaint).

²²⁰ *Id.* at 623. It is not exactly clear from the language of the decision whether the city council tried to make a personal jurisdiction objection or subject matter objection. On the one hand, an assertion that the court’s review is limited to application of a certain law more resembles a subject matter challenge. When a party agrees to litigate in a certain jurisdiction or limits such an agreement to a certain jurisdiction, however, such an agreement is enforceable and relevant only to questions of personal jurisdiction.

²²¹ *Id.* at 623.

the decision, the court concluded that the only possible significance of a previous UDRP process in this context was that it triggered the RDNH provision.²²² Furthermore, the court concluded that it was not limited in any way by the WIPO proceeding and the law applied there.²²³ In sum, the federal court had jurisdiction over the City Council and over the dispute, and the UDRP decision, including the law applied under the procedure, had no bearing on the federal court's jurisdictional reach and legal analysis.

2. Foreign Law Not Applicable

In the second part of the analysis, the court gave no deference to Spanish law and determined that the district court erred in analyzing the parties' rights under a foreign legal system.²²⁴ The RDNH provision provides a cause of action to the losing registrant and allows a plaintiff to show in federal court that the registration is "not unlawful under this chapter."²²⁵ The chapter being referred to is chapter 22 of title 15 of the U.S. Code, which contains the Lanham Act; and foreign law was not applicable.²²⁶

3. The Elements of the RDNH Provision

Third, the court enumerated the elements of the section 1114(2)(D)(v) cause of action, finding each to be present in this case. Under the statute, plaintiff must show that (1) he or she is the domain name registrant; (2) his or her domain name was suspended, disabled or transferred under a policy implemented by the registrar (here, the UDRP); (3) that the owner of the mark had a notice of the action in federal court and; (4) that plaintiff's

²²² *Id.* at 625.

²²³ *See id.* at 626.

²²⁴ *Id.* at 627.

²²⁵ *Barcelona.com*, 330 F.3d at 627 (quoting 15 U.S.C. § 1114(2)(D)(v) (2000)). The *Barcelona.com* court noted that the original language of ACPA provides that the registrant may sue to declare that the domain name's use by such registrant is "not unlawful under this Act," with "Act" defined to refer to the Trademark Act of 1946 (the Lanham Act). *Id.* at 627 n.2 (citing 113 Stat. 1501A-550, § 3004 (1999)). But upon codification, the term "this Act" became "this chapter," i.e., chapter 22 of title 15, which contains the Lanham Act. *Barcelona.com*, 330 F.3d at 627 n.2.

²²⁶ *See Barcelona.com*, 330 F.3d at 627 & n.2.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 69

registration or use of the domain name is not unlawful under the Lanham Act, as amended.²²⁷ Since the first three elements of the test were undisputed and since the City Council did not even attempt to prove trademark rights in the term Barcelona under U.S. law, the court determined that Barcelona.com, Inc. was entitled to the protection of the RDNH provision.²²⁸

4. BARCELONA Is Not a Protected Mark in the United States

Fourth and last, the court explained that even had the City Council tried to defend its trademark rights in the term Barcelona under U.S. law, it would have been of no avail. Because the Lanham Act did not protect purely descriptive-geographical designations,²²⁹ and because the City Council could show no evidence that the name Barcelona acquired any secondary meaning other than the city itself, the term was not protected under U.S. law.²³⁰

IV. ANALYSIS AND PROBLEMS IN THE PRESENT STATE OF THE LAW

This part, divided into five sections, further analyzes the court's opinion and explores its possible consequences. Section A explains why the *Barcelona.com* court probably rendered a correct application of ACPA under the circumstances. Section B discusses and criticizes the opinion's territoriality justification for the result. Subsection C reviews some emerging litigation strategies and the development of a "partial reverse effect" pushing owners of foreign marks away from UDRP and back to litigation in foreign courts. Section D describes the outcome of *Barcelona.com* in the

²²⁷ *Id.* at 626.

²²⁸ *Id.* at 626–29.

²²⁹ *Id.* at 628–29 (citing 15 U.S.C. § 1052(e)(2) (2000)).

²³⁰ *Id.* at 629. Additionally, the Fourth Circuit in *Barcelona.com* briefly addressed the district court's discussion of the city's counterclaims of an ACPA violation by the plaintiff-registrant. The circuit court found that the city had never filed a counterclaim and thus vacated the rulings that arose from the "phantom counterclaim." *Id.* at 629; *see also infra* note 262.

context of other court decisions, attempting to convey the larger context of contemporary cybersquatting jurisprudence in the United States. This section classifies recent ACPA case law into three categories having particular relevance in international disputes. It further highlights the “laundry machine effect” and its paradox, a troublesome aspect of current ACPA interpretation. Finally, Section E discusses the implications of current cybersquatting jurisprudence for owners of foreign marks and some possible foreign reactions to that legal landscape.

A. *Correct Application of the Law*

The two major innovations of the *Barcelona.com* case in the field of domain name disputes are probably the following: (1) the *Barcelona.com* court was the first appellate court to state and clarify the elements of the RDNH cause of action; and (2) it concluded that courts should look only to U.S. law to determine whether a registration is lawful.

It seems that the *Barcelona.com* court’s legal analysis is technically correct. With respect to the principal controversy between the parties, the language of ACPA is clear and straightforward. The RDNH provision²³¹ explicitly provides the law under which registration should be scrutinized in a RDNH situation—“the registration or use . . . is not unlawful under *this chapter*.”²³² Additionally, ACPA was mainly crafted by the U.S. Congress to protect U.S. marks in U.S. federal courts.²³³ Therefore, the RDNH provision applies the U.S. standard for unlawful cybersquatting.²³⁴ A conclusion that the provision mandates analysis under foreign system would give U.S. courts subject matter jurisdiction to adjudicate marks recognized by every

²³¹ 15 U.S.C. § 1114(2)(D)(v) (2000).

²³² *Id.* (emphasis added); *see supra* note 225.

²³³ Senator Spence Abraham of Michigan, one of the Congressional sponsors of the ACPA, stated, “This legislation will combat a new form of high tech fraud that is causing confusion and inconvenience for consumers . . . and posing an enormous threat to a century of pre-Internet *American* business efforts.” 145 CONG. REC. S7334 (daily ed. June 21, 1999) (statement of Sen. Abraham) (emphasis added).

²³⁴ An example of an alternative standard could be found in UDRP, *supra* note 98, ¶ 4(a). *See also* discussion *supra* Part II.A.1 (describing the UDRP cybersquatting standard).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 71

possible trademark regime of any country.²³⁵ In other words, such a reading would effectively render ACPA a kind of conduit, bringing validity questions of all world marks under the scrutiny of U.S. courts—a result that would be at odds with common sense.²³⁶

B. *The Territoriality Argument*

It is interesting to observe the emphasis the court put on territoriality in trademark law. In part III of the *Barcelona.com* decision, which reinforced the Fourth Circuit's opinion about the exclusive application of U.S. law, the court noted²³⁷ that both the United States and Spain have been longtime members of the Paris Convention of 1883.²³⁸ The Paris Convention recognizes the independence of trademark rights among its member states.²³⁹ Furthermore, the Paris Convention does not grant greater protection in the United States to foreign marks than what is already secured under the Lanham Act.²⁴⁰

This is probably an accurate statement of the law, although slightly flawed. The problem derives from the attempt to justify a certain reading of the ACPA using traditional territoriality principles. As noted earlier, U.S. trademark law aims to prevent confusion and unlawful commercial competition practices. In

²³⁵ Interestingly, the ACPA uses different language regarding the trademarks falling under its various provisions. The ACPA in rem provision specifically limits its applicability to registered U.S. marks and those marks protected under Lanham Act dilution and infringement provisions. See 15 U.S.C. § 1125(d)(2)(A)(i). The language of the in personam provision plainly protects “a mark.” See *id.* § 1125(d)(1)(A). Similarly, it appears that the language of the RDNH provision refers to a “mark owner” (against whom this provision can be exercised) without further specifications. See also *infra* note 262 and accompanying text.

²³⁶ See discussion *infra* Part IV.D.4 (arguing that the *Barcelona.com* court reached the only reasonable result under the circumstances).

²³⁷ *Barcelona.com*, 330 F.3d at 628.

²³⁸ Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, as amended at Stockholm, July 14, 1967, 21 U.S.T. 1583 [hereinafter Paris Convention].

²³⁹ Article 6(3) of the Paris Convention secures the territorial independence of marks, thus allowing every member-state discretion whether to grant protection within its territory to foreign marks protected in other member states. See Paris Convention, *supra* note 238, art. 6(3), noted in *Barcelona.com*, 330 F.3d at 628.

²⁴⁰ See *Barcelona.com*, 330 F.3d at 628 (citing *Scotch Whisky Ass'n v. Majestic Distilling Co.*, 958 F.2d 594, 597 (4th Cir. 1992); *Int'l Cafe, S.A.L. v. Hard Rock Cafe Int'l (U.S.A.), Inc.*, 252 F.3d 1274, 1278 (11th Cir. 2001)).

many cases, trademark protection, while securing private monopolies that grant exclusive use of certain marks by certain commercial players, may be justified only if applied within a certain territory where those commercial practices are potentially harmful. For example, when courts and commentators talk about likelihood of confusion it is clear that such confusion may occur only where consumers recognize the mark as a source identifier.²⁴¹ In other words, in order to be protected in a particular jurisdiction, a mark must meet that jurisdiction's legal tests for protection. In some jurisdictions, this means executing the formalities of registration. Meanwhile, in the U.S. federal system the crux is the use in U.S. commerce requirement.²⁴²

Hence, trademark law can be described as territorial. The digital-commercial reality introduced new challenges to this territoriality concept; thus, the ACPA was enacted to address these challenges.²⁴³ One of the act's responses to those challenges was the relinquishment of the likelihood of confusion requirement,²⁴⁴ a highly territory-sensitive element of trademark protection. Furthermore, the ACPA imposes liability without a showing that the domain name was used in commerce at all.²⁴⁵ The former *sine qua non* concept of use in commerce as an essential element of any trademark infringement or dilution claim in the United States is

²⁴¹ See MCCARTHY ON TRADEMARKS, *supra* note 66, § 29:4, at 29-10 (noting that foreign marks famous in the United States "should be legally recognized in the United States").

²⁴² See *United Drug Co. v. Theodore Rectanus Co.*, 248 U.S. 90, 97 (1918) ("[T]he right to a particular mark grows out of its use."). The opinion further discusses geographic scope of use-based rights. See *id.* at 97-104.

²⁴³ See discussion *supra* Part I.C (explaining why "offline" trademark law failed to effectively protect marks in online activities).

²⁴⁴ The ACPA in personam provision replaced that test with the "identical or confusingly similar" test, 15 U.S.C. § 1125(d)(1)(A) (2000), which arguably bears much lower burden of proof than "likelihood of confusion." See, e.g., *Morrison & Foerster, LLP v. Wick*, 94 F. Supp. 2d 1125, 1130 (D. Colo. 2000). The in personam provision also imposes liability "without regard to the goods or services of the parties." 15 U.S.C. § 1125(d)(1)(A).

²⁴⁵ ACPA does not include a requirement of "use in commerce" for in personam actions. In rem actions, however, are subject to the traditional limitations of the trademark infringement and dilution statutes. See 15 U.S.C. § 1125(d)(2)(A)(i).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 73

also territory sensitive.²⁴⁶ Both the likelihood of confusion and use in commerce requirements were abandoned by the ACPA's in personam provisions, *inter alia*, because those traditional concepts dictated territorial protection that was insufficient in the context of the Internet.

As explained earlier, domain names are both unique and have global reach. They are unique in that only one entity can register a single domain name worldwide. Global reach means that domain names are instantly, cheaply, and simultaneously accessible and recognizable by Internet users all over the world, without territorial boundaries or limitations. These characteristics of domain names had a major influence on the formulation of the ACPA, including its RDNH provision. In sum, trademark territoriality theory provides a good explanation why U.S. law, and only U.S. law, should determine trademark rights and protection in U.S. territory. When the question is why should U.S. law, and only U.S. law, determine trademark protection of a Spanish mark that is arguably infringed on Spanish soil, the territoriality theory does not furnish the most satisfactory reasoning.

C. Emerging Litigation Strategies

Generally speaking, after more than three years of intensive litigation where the ACPA was heavily used against abusive registrants and registrations, it is now safe to say that this U.S. legislation virtually eliminated the benefits of cybersquatting in gTLDs to classic cybersquatters such as Toeppen²⁴⁷ and Zuccarini.²⁴⁸ Assuming the rulings of the Fourth and the First Circuits in *Barcelona.com* and *Sallen*, respectively, survive the rapid changes and evolution of technology and technology-related law, it should also be relatively safe for losing registrants to rely on the RDNH cause of action where the registration is determined not to violate U.S. law. Consequently, registrants can protect their domain name registrations in U.S. courts from the fast and unpredictable UDRP process, where a panel can decide a dispute

²⁴⁶ See *supra* note 78 (listing prominent examples of the "use in commerce" requirement in the Lanham Act).

²⁴⁷ See, e.g., *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

²⁴⁸ See, e.g., *Shields v. Zuccarini*, 254 F.3d 476 (3d Cir. 2001).

“in accordance with the Policy, these Rules and *any rules and principles of law that it deems applicable.*”²⁴⁹ After the *Barcelona.com* decision, federal courts are expected to decide on RDNH provision actions by taking into consideration only marks that are recognized under U.S. trademark law. Hence, it becomes clear that a mark owner, whose rights in the mark are recognized *only* by a foreign system, will almost automatically lose in RDNH provision actions. This alarming consequence calls for further discussion in possible litigation strategies.²⁵⁰

1. The Registrant’s (Probably) Winning Strategy

Suppose that you are a prospective registrant contemplating registration of a certain domain name, for example, <www.schlecker.com>.²⁵¹ You are aware that there is a foreign mark (i.e., a non-U.S. protected mark) incorporated and held by a foreign commercial entity called Schlecker.²⁵² You envision a possible dispute, and since a UDRP action is usually more attractive to mark owners than court litigation, it is more likely that the troubles will come from a UDRP complainant attacking your registration.²⁵³

In order to maximize your chances of keeping the domain name, you may implement a simple strategy: choose a U.S. registrar with its principal office in the United States and register

²⁴⁹ UDRP RULES, *supra* note 106, ¶ 15(a) (emphasis added).

²⁵⁰ Litigation strategies refer generally to the behavior of parties before and during litigation which is intended to increase their chances of winning in court.

²⁵¹ It should be noted at the outset that this hypothetical does not speculate on your specific mens rea (i.e., the existence of bad faith or other types of mental state). This is to avoid sensitivity of the hypothetical to different cybersquatting standards. The hypothetical assumes that you are only *aware* of the existence of the foreign mark, no more and no less.

²⁵² For purposes of this hypothetical, one is aware that Schlecker is the name of a famous drugstore retailer chain in Germany. The good news is, however, that Schlecker is not a registered mark in the United States, engages in no commercial activity, and does have a single American shop. Additionally, the name is not generally familiar to U.S. consumers. The better news, however, is that Schlecker neglected to register the domain <http://www.schlecker.com> before you came up with the idea.

²⁵³ See *supra* Part II.A.1 (discussing UDRP and its attractiveness to mark owners). This assertion is especially valid in an international dispute, involving parties and rights from both sides of the Atlantic.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 75

your domain name, making sure the owner of the registration is a U.S. entity with a U.S. address to appear in the registrar's Whois database.²⁵⁴ Next, wait for the UDRP complaint to arrive and when it does, defend your registration in the UDRP process.²⁵⁵ If you win the UDRP proceeding²⁵⁶ and the mark owner decides not to challenge the result in court, the domain name is yours.²⁵⁷

Conversely, if you lose under the UDRP, then file a RDNH provision suit in a U.S. federal court of mutual jurisdiction against that mark owner within ten business days. As explained above, upon such filing the cancellation or transfer of your domain name will have an automatic stay until the matter is resolved in court or otherwise.²⁵⁸ The mark owner will have difficulty objecting to the court's personal jurisdiction, since upon filing the UDRP complaint he or she agreed to submit to a court of mutual jurisdiction in adjudicating disputes concerning the domain name.²⁵⁹ Thus, the mark owner is arguably locked into the federal

²⁵⁴ It appears that your own citizenship or domiciliary is irrelevant for the success of the strategy.

²⁵⁵ You should remember to strictly comply with the procedural UDRP Rules, particularly with the rule 5(a) requirement of a timely response, as well as with the other rule 5 guidelines for submitting a response. See UDRP RULES, *supra* note 106, ¶ 5.

²⁵⁶ Registrants, however, have a statistically better chance to lose a UDRP process than to win it. See Michael Geist, *Fundamentally Fair.com? An Update on Bias Allegations and the ICANN*, at <http://aix1.uottawa.ca/~geist/fairupdate.pdf> (last visited Nov. 3, 2003) (examining 4,332 early UDRP decisions and finding that registrants statistically lose in a significant majority of the cases); see also Milton Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute*, Digital Convergence Center, at <http://dcc.syr.edu/reports.htm> (finding that registrants lost in almost 80 percent of the UDRP decision rendered in its first year of implementation) (Nov. 2000).

²⁵⁷ Mark owners, as well as registrants, may challenge UDRP decisions in a court of competent jurisdiction: "The mandatory administrative proceeding requirements . . . shall not prevent either you or the complainant from submitting the dispute to a court of *competent jurisdiction* for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded." UDRP, *supra* note 98, ¶ 4(k) (emphasis added). A definition of "competent jurisdiction," however, can be found neither in the Policy nor in the UDRP Rules.

²⁵⁸ UDRP, *supra* note 98, ¶ 4(k).

²⁵⁹ In its *Barcelona.com* opinion, the Fourth Circuit chronicled the district court's proceedings in response to "the City Council's argument that 'failure to consider the basis for the [WIPO] decision would remove the basis for [this court's] jurisdiction.'" See *Barcelona.com*, 330 F.3d at 623. The court stated:

[Barcelona.com, Inc.'s] complaint, brought in the Eastern District of Virginia . . . originally asserted three claims in three separate counts: a claim

court, no matter what connection he or she has with the forum.²⁶⁰ Since the mark owner has only foreign trademark rights to vindicate, you may expect an almost certain victory in the federal court.²⁶¹

A possible wrinkle in this strategy appears when the mark owner launches a less typical offensive—skipping UDRP and suing you in court for trademark infringement or dilution. Again, assuming no U.S. trademark rights are involved, the ACPA as applied by a U.S. court would probably leave mark owners with no recourse.²⁶² If sued in a foreign court, however, with or without a

for declaratory judgment and injunctive relief under 15 U.S.C. § 1114(2)(D)(v); a claim for fraud and unfair competition; and a claim for tortious interference with prospective economic advantage. In response to the City Council's motion to dismiss on various jurisdictional grounds, [*Barcelona.com, Inc.*] voluntarily dismissed all claims except its claim under § 1114(2)(D)(v). After the district court denied the City Council's motion to dismiss, the City Council filed an answer, stating as one of its affirmative defenses:

This court lacks jurisdiction over Defendant for any cause of action other than Plaintiff's challenge to the arbitrator's Order issued in the UDRP domain name arbitration proceeding.

Id. (emphasis added). It may be reasonable to assume that even *Barcelona.com, Inc.* believed, already in an early stage of litigation, that its only real chance to assert jurisdiction was through the application of the RDNH provision. This aspect of the case also illustrates the city's confusion regarding the difference between personal jurisdiction and subject matter jurisdiction. *See supra* note 220.

²⁶⁰ In fact, the chief director of the city council "submitted an affidavit stating that "[t]he City does not own and is not using any trademarks in the United States, to identify any goods or services." *Barcelona.com*, 330 F.3d at 629.

²⁶¹ *But see* *McNeil v. Stanley Works*, No. 00-16557, 2002 U.S. App. LEXIS 6762, at *3 (9th Cir. Apr. 10, 2002) (doubting the contractual enforceability of a UDRP complainant's forum choice with respect to challenges of UDRP decisions) (dictum).

²⁶² The ACPA's in rem provision specifically includes only those marks protected under the Lanham Act against infringement or dilution or registered in the Patent and Trademark Office. *See* 15 U.S.C. § 1125(d)(2)(A)(i) (2000). The ACPA's in personam provision more broadly covers "mark[s]." *See id.* § 1125(d)(1)(A). "Mark" is defined in the Lanham Act as "any trademark, service mark, collective mark, or certification mark." *Id.* § 1127. Additionally, the *Sallen* decision indicates that the term "mark owner" as used in the RDNH provision covers not only U.S. marks, but also any trademark. *See Sallen v. Corinthians Licenciamentos LTDA*, 273 F.3d 14, 24 (1st Cir. 2001) (citing 15 U.S.C. § 1114(2)(D)(v)). Accordingly, owners of foreign marks may arguably bring ACPA in personam actions in U.S. courts. Since the *Sallen* decision is an RDNH decision and not an in personam decision, however, the author assumes that the holding is binding only in that context, although a more expansive reading is plausible. For example, the *Barcelona.com* district court, discussing possible counterclaims of the city council, concluded that the ACPA in personam provision protected foreign marks. *See*

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 77

preceding UDRP process, you should fiercely object to that court's jurisdiction. If the challenge fails, you may need to prove legitimate use of the registration according to that jurisdiction's rules.²⁶³

Finally, even if you lose in the foreign court and that court issues an order in favor of the mark owner, it is not over yet. You may still eventually prevail in a U.S. federal court. To date, there is at least one such example: a federal district court ordered Verisign—which was the domain name registry—to ignore a Korean court decision ordering the Korean registrar not to transfer a domain name.²⁶⁴

2. The Foreign-Mark Owner's (Probably) Losing Strategy

Now imagine yourself in the shoes of the hypothetical Schlecker (i.e., the owner of a foreign mark having its mark registered by a sophisticated registrant). The best strategy is to skip the UDRP and sue directly where the mark is protected.²⁶⁵ The reason is rather straightforward: the foreign mark owner knows that even if it wins under the UDRP, it may be forced to

Barcelona.com, Inc., v. Excelentísimo Ayuntamiento de Barcelona, 189 F. Supp. 2d 367, 373–374 (E.D. Va. 2002), *rev'd and vacated*, 330 F.3d 617. The Fourth Circuit, however, vacated this finding, concluding that the city never filed such counterclaims. 330 F.3d at 629. Thus, this issue remains open.

²⁶³ Notice, however, that international jurisdictions would probably have to adjudicate the dispute according to traditional trademark law and some newly evolved doctrines created to deal with cybersquatting. Thus far, it seems the United States is alone in legislating such a powerful tool against cybersquatting as the ACPA. *See Sharrock, supra* note 17, at 826–27 (comparing cybersquatting remedies available in U.S. courts to those available outside the United States). *But see infra* notes 331, 344 (noting Japan's cybersquatting protection).

²⁶⁴ *See GlobalSantaFe Corp. v. Globalsantafe.com*, 250 F. Supp. 2d 610, 625 (E.D. Va. 2003) (finding that the Eastern District of Virginia was first in asserting in rem jurisdiction over the disputed domain name and concluding that the physical location of the registry in Virginia furnishes sufficient basis to assert in rem jurisdiction even though the registrar was located in Korea). Although this was an in rem case with a peculiar set of circumstances, as distinguish from the RDNH hypothesis, it is still relevant to illustrate the following point: foreign courts' power to effectuate their decisions is very limited compared to that of U.S. courts, sitting where registries typically reside. When the door to a U.S. court is potentially opened before a losing party in a former, foreign proceeding, that court is not, *arguendo*, the final arbiter of the dispute.

²⁶⁵ In this case, a mark owner would probably want to sue in Germany, where the mark is established.

later litigate in the United States, where it would probably lose.²⁶⁶ On the other hand, if you find yourself in the shoes of the City Council of Barcelona, and you are already compelled to litigate in a U.S. court under the RDNH provision, your best strategy is probably to put all your efforts into strenuously objecting to the U.S. court's in personam jurisdiction.²⁶⁷ You should do so despite the fact that you have already submitted to the U.S. court in the UDRP filing.²⁶⁸ If you fail in the jurisdictional stage, try to assert some protected rights under the Lanham Act, such as common law trademark rights.²⁶⁹ Obviously, once in federal court, you are in a much worse position than your opponent. In fact, in light of the *Barcelona.com* decision, you have almost no hope there at all.

3. The Partial Reverse Effect

As mentioned, the UDRP brings the domain name dispute under the RDNH provision of the ACPA.²⁷⁰ The term "partial reverse effect" refers to a potential, new trend among owners of foreign marks to prefer foreign litigation and skip the UDRP option.²⁷¹ It is only a "partial" effect because the UDRP remains attractive to U.S. mark owners. The motivation for the effect is that the UDRP becomes a trap, possibly forcing owners of foreign

²⁶⁶ Indeed, the Fourth Circuit in *Barcelona.com* indicated that a possible effect of an earlier UDRP proceeding would be to bring the dispute under the scope of the RDNH provision of the ACPA:

[T]he ACPA authorizes a suit by a domain name registrant whose domain name has been suspended, disabled or transferred under that reasonable policy (including the UDRP) to seek a declaration that the registrant's registration and use of the domain name involves no violation of the Lanham Act as well as an injunction returning the domain name.

Barcelona.com, 330 F.3d at 625 (emphasis removed). Absent such stage, the RDNH is probably inapplicable by its own terms.

²⁶⁷ This is assuming that the RDNH provision actually requires this type of territorial jurisdiction. See *supra* discussion in Part II.B.3. A subject-matter jurisdiction objection would probably not be convincing in light of *Sallen*.

²⁶⁸ The hardship of convincing a court to accept such a problematic assertion is evident on its face.

²⁶⁹ See, e.g., *Emergency One, Inc. v. Am. Fire Eagle Engine Co.*, 332 F.3d 264, 267–69 (4th Cir. 2003) (providing an overview on common law trademark rights and citing relevant authorities).

²⁷⁰ See *supra* note 266 and accompanying text.

²⁷¹ Especially in light of the litigation hurdles waiting for them in U.S. courts. See discussion *supra* Part IV.C.2.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 79

marks to litigate where they are very likely to lose.²⁷² In other words, a possible cheap and fast victory under UDRP may lead to an expensive and extremely risky proceeding in a U.S. court. The anticipated partial reverse effect might have a substantial adverse impact on the concept and function of UDRP. A policy that is attractive only to U.S. mark owners may pose difficult legitimacy questions.²⁷³ In addition, the partial reverse effect may increase the volume of international domain name litigation, leading to conflicting decisions and posing a difficult test to the comity concept as applied by various courts.²⁷⁴ In sum, a partial reverse effect is something to avoid and inhibit, especially if one believes that UDRP was essentially a good idea.

D. The Big Picture and Its Critique

In order to fully grasp the implication of the *Barcelona.com* decision, it is necessary to have a broader perspective of other recent, important case law, creating together the big picture of cybersquatting law in the United States. Some of the most troubling issues encountered by courts applying the ACPA in international domain name disputes were due process, the extraterritorial effect, and the international comity problems. This section briefly describes these problems and the ways U.S. courts dealt with the new challenges.

1. Minimum Contacts Yes or No; What Does *Shaffer* Really Mean?

U.S. courts generally found no minimum contacts sufficient to establish personal jurisdiction resulting from mere online presence

²⁷² *See id.*

²⁷³ Indeed, UDRP legitimacy questions have already bothered commentators and invoked harsh criticism even without considering the described reverse effect. *See, e.g.*, Froomkin, *supra* note 16 (critiquing the formation and use of ICANN as means to avoid proper public rulemaking); A. Michael Froomkin & Mark A. Lemley, *ICANN and AntiTrust*, 2003 U. ILL. L. REV. 1 (describing economic-competitive aspects of ICANN functions and its relationship with the U.S. government); Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2000).

²⁷⁴ See discussion on international comity *infra* Part IV.D.3.

of the defendant that could be accessed in that jurisdiction.²⁷⁵ Additionally, minimum contacts generally could not be established by mere registration of the domain name with a registration authority located in the jurisdiction.²⁷⁶ Therefore, personal jurisdiction over alleged cybersquatters was often very hard to establish.²⁷⁷ The alternative was in rem jurisdiction.²⁷⁸

Part I.B.2 of this Article provided a brief description of the three types of in rem jurisdiction. The first type is true in rem jurisdiction, relevant when the action is concerning rights in a res located in the jurisdiction of plaintiff against the world, i.e., against any potential, non-specified right holder.²⁷⁹ Thus, in rem jurisdiction that determines the exclusive rights to use a certain domain name has a true in rem effect.²⁸⁰ In *Shaffer v. Heitner*, the Supreme Court was asked to resolve a question of quasi in rem II (sometimes called attachment) jurisdiction.²⁸¹ The *Shaffer* court

²⁷⁵ See discussion *supra* Part I.B.1; see also *Shri Ram Chandra Mission v. Sahajmarg.org*, 139 F. Supp. 2d 721, 722 (E.D. Va. 2001) (noting the dismissal of the original in personam action due to lack of minimum contacts with the jurisdiction when the only contact was mere registration).

²⁷⁶ *Am. Online, Inc. v. Huang*, 106 F. Supp. 2d 848, 859 (E.D. Va. 2000) (finding that registration of the domain name in Virginia alone was not sufficient to establish minimum contacts with Virginia for establishing in personam jurisdiction).

²⁷⁷ See discussion *supra* Part II.B.1; see also *Porsche Cars N. Am., Inc. v. Porsch.com*, 51 F. Supp. 2d 707, 709–10 (E.D. Va. 1999) (plaintiff in a pre-ACPA case attempted to bring an in rem action against the domain names instead of an in personam action against the registrants), *vacated due to a superseding statute* by *Porsche Cars N. Am., Inc. v. Allporsche.com*, 215 F.3d 1320 (4th Cir. 2000) (table), and *remanded in part* by *Porsche Cars N. Am., Inc. v. Porsche.net*, 302 F.3d 248 (4th Cir. 2002).

²⁷⁸ See *Porsche Cars*, 51 F. Supp. 2d at 709–10.

²⁷⁹ See RESTATEMENT (SECOND) OF JUDGMENTS § 6 cmt. a (1982) (noting that in a true in rem proceeding, but not necessarily in a quasi in rem proceeding, the judgment is binding even on persons to whom no notice of the proceeding was given).

²⁸⁰ *CNN I*, 162 F. Supp. 2d 484, 491 (E.D. Va. 2001) (categorizing a domain name jurisdiction action as “true in rem,” where the owner of the res need not have minimum contacts with the forum).

²⁸¹ 433 U.S. 186, 189 (1977). The question there was whether a Delaware statute allowing in rem jurisdiction through sequestration of Delaware corporation shares owned by a non-resident defendant in order to compel personal appearance in an unrelated claim was constitutional. See *id.* at 189–95. In the case, a shareholder brought a derivative action against the non-resident shareholder of a Delaware corporation in a matter unrelated to the rights in the shares. *Id.* at 189–92. Because the Delaware statute afforded an in rem action determining the rights of the parties unrelated to the “location” of the shares, this was a quasi in rem II (or “attachment”) case.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 81

ruled that the Delaware statute providing attachment jurisdiction against a non-resident shareholder of a Delaware corporation must satisfy the minimum contacts standard of due process.²⁸²

The controversy over the correct interpretation of *Shaffer* in the context of domain names disputes can be reduced to whether the minimum contacts standard also applies to true in rem jurisdiction—and thus also to the ACPA in rem provision—or whether minimum contacts are required solely in quasi in rem II jurisdictions. Struggling with this question, courts generally have upheld the ACPA in rem actions even when the rights of a person having no minimum contacts with the jurisdiction were affected.²⁸³ Such application of the ACPA was justified by viewing as mere dicta statements in *Shaffer* which arguably require a more expansive application of the minimum contacts requirement to include all types of in rem actions.²⁸⁴

2. The Extraterritorial Effect of the ACPA

An extraterritorial application of domestic trademark law is a problem, as trademark law is territorial and each sovereign should be free to provide protection within its territory according to its

²⁸² *Id.* at 207 (citing *Int'l Shoe v. Washington*, 326 U.S. 310 (1945)).

²⁸³ See *CNN I*, 162 F. Supp. 2d 484, 491 (E.D. Va. 2001). The court stated: [W]here, as here, the action is properly categorized as “true in rem,” there is no requirement that the owner or claimant of the res have minimum contacts with the forum. More particularly, in an ACPA in rem action, it is not necessary that the allegedly infringing registrant have minimum contacts with the forum; it is enough, as here, that the registry is located in the forum.

Id. See also *CNN II*, 177 F. Supp. 2d 506, 527 (E.D. Va. 2001) (asserting jurisdiction by virtue of the deposit of the certificate of registration by the registrar with the court as establishing in rem jurisdiction and taking a narrow reading of *Shaffer*); *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214, 225 (4th Cir. 2002) (upholding the constitutionality of the ACPA in rem provision); *CNN Appeal*, No. 02-1112, 2003 WL 152846, at *3 (4th Cir. Jan. 23, 2003) (citing *Harrods*, 302 F.3d at 225).

²⁸⁴ See, e.g., *Shaffer*, 433 U.S. at 209. The court stated:

Thus, although the presence of the defendant's property in a State might suggest the existence of other ties among the defendant, the State, and the litigation, the presence of the property alone would not support the State's jurisdiction. If those other ties did not exist, cases over which the State is now thought to have jurisdiction could not be brought in that forum.

Id.

own domestic rules.²⁸⁵ The guiding Supreme Court opinion on the issue of extraterritorial application of the Lanham Act is *Steele v. Bulova Watch Co.*²⁸⁶ The *Bulova* Court, acknowledging the problematic aspect of applying the Lanham Act in disputes involving extraterritorial effect, held that such an application was appropriate only where the infringing activity adversely affects U.S. commerce.²⁸⁷ In essence, the *Bulova* decision dictates that extraterritorial application of U.S. trademark law is appropriate only when (1) defendant is a U.S. citizen (or has extensive contacts and presence in the United States); (2) defendant's conduct (in a foreign country) affects U.S. commerce; and (3) there is no conflict between U.S. law and the foreign country's law as a result of applying the Lanham Act.²⁸⁸

The relevance of the extraterritorial effect doctrine is evident in cases of international domain name disputes, where application of the ACPA has immediate international effects. Clearly, a U.S. court imposing the ACPA rules in a gTLD dispute determines what each and every Internet user in the world will see—or will not see—when clicking the corresponding Internet address. At the same time, such court has control over the availability of domain name registrations to foreign actors, regardless of their nationality or contacts with the U.S. forum. The problem is especially acute in applying the in rem provision absent of any of the extraterritoriality doctrine constraints.²⁸⁹

U.S. courts, evaluating the extraterritorial effects of their ruling in domain name disputes, generally do not consider such effects as a constraint. For example, the federal court for the Eastern District of Virginia, in its second opinion in the *Cable News Network L.P.*

²⁸⁵ See *supra* Parts I.C.1, IV.B (discussing the territoriality concepts in trademark law).

²⁸⁶ 344 U.S. 280 (1952).

²⁸⁷ See *id.* at 285–87.

²⁸⁸ See *Vanity Fair Mills v. T. Eaton Co.*, 234 F.2d 633, 642–43 (2d Cir. 1956) (analyzing *Bulova*); see also Xuan-Thao N. Nguyen, *The Digital Trademark Right: A Troubling New Extraterritorial Reach of United States Law*, 81 N.C. L. REV. 483, 492–500 (2003) (analyzing *Bulova*, *Vanity Fair*, and U.S. jurisprudence regarding extraterritorial effect doctrine).

²⁸⁹ See Nguyen, *supra* note 288, at 544–45 (enumerating the extraterritoriality doctrine's limitations and noting that none of them exist in the ACPA in rem provision).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 83

v. CNNNews.com case (“*CNN II*”),²⁹⁰ concluded that <www.cnnnews.com>—a Chinese news Web site which registered with a Chinese registrar²⁹¹ that displayed text almost entirely in the Chinese language, offered no goods for sale outside China, and was ostensibly directed solely at Internet users outside of the United States—constituted use in U.S. commerce and affected U.S. commerce.²⁹² The court’s reasoning for this conclusion was quite remarkable. First, the court found that the Chinese Web site’s “effect or impact” on U.S. commerce “results from the global nature of the Internet.”²⁹³ Second, the court concluded that “.com” is essentially an *American* top-level domain.²⁹⁴ Thus, the Chinese Web site was offering news services in the United States, and because the Cable News Network (“CNN”) was a famous mark in America, U.S. commerce was affected.²⁹⁵ The result suggests that the extraterritoriality doctrine does not stop U.S. courts from applying the Lanham Act in gTLD registrations. While one court further expressed the worry that U.S. marks would

²⁹⁰ See *CNN II*, 177 F. Supp. 2d 506 (E.D. Va. 2001). The district court issued two opinions in this case, the first of which denied a dismissal and the second of which granted summary judgment to the plaintiff, Cable News Network L.P.

²⁹¹ After the controversy over the Web site had arisen, but before the plaintiff filed its complaint, the defendant changed the registrar from NSI, a U.S. firm, to Eastern Communication Company Ltd., a Chinese registrar. See *CNN II*, 177 F. Supp. 2d at 514.

²⁹² *Id.* at 517–18.

²⁹³ *Id.* at 517.

²⁹⁴ *Id.* (emphasis added) (footnote omitted).

²⁹⁵ *Id.* at 517–18. Some other courts followed this approach. See, e.g., *Am. Online, Inc. v. Aol.org*, 259 F. Supp. 2d 449, 456 (E.D. Va. 2003). The court stated:

Yet, this is not an “extraterritorial application” of the Lanham Act or the ACPA, because [Public Interest Registry], the “.org” registry, is located in this district, and the transfer order would not “specifically enjoin any activity outside the United States; instead, [the order] would be limited to ordering [the registry] in this [district] to transfer ownership of [the] domain name.”

Id. (quoting *CNN II*, 177 F. Supp. 2d at 518 n.29); see also *Internet Billions Domains, Inc. v. Venetian Casino Resort, L.L.C.*, No. 01-5417, 2002 U.S. Dist. LEXIS 11805 (E.D. Pa. May 31, 2002). In *Internet Billions*, the court found that “the mere fact that the internet allows for worldwide access does not strip an American court of its subject matter jurisdiction under the Lanham Act over activities directed at the United States.” *Id.* at *16. The court continued: “As the ‘.org’ suffix with no country code in the domain name for a Web site that uses English has been held to target users in the United States, we find the allegations that [plaintiff’s] activities were directed toward the United States to be sufficient.” *Id.* (citing *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L’Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001)).

be infringed without recourse by using foreign registries such as ccTLD,²⁹⁶ another had the practical advice for foreign registrants who think that the U.S. process is unfair—register with a ccTLDs in the first instance.²⁹⁷

3. International Comity Considerations

The extraterritorial effect doctrine is one manifestation of a more general concept of international comity.²⁹⁸ The fundamental assumption of comity is the recognition by one legal system applying its law in its territory of the potential involvement of interests of other sovereign's law system.²⁹⁹ A relevant aspect of comity "ordinarily requires that courts of a separate sovereign not interfere with concurrent proceedings based on the same transitory

²⁹⁶ See *GlobalSantaFe Corp. v. Globalsantafe.com*, 250 F. Supp. 2d 610, 624 (E.D. Va. 2003). The court stated:

[A] desire to avoid United States jurisdiction may cause foreign registrants to choose to use domain names within their respective country code top-level domains, whose registries are located in and operated by the foreign countries, rather than the currently popular 'generic' domain names such as ".com" and ".net." The result may be an increasing number of domain names registered out of the reach of United States jurisdiction, but accessible to United States users through the universal domain name system, which in turn will pose a serious challenge to the enforcement of United States trademark rights on the Internet.

Id.

²⁹⁷ See *Am. Online*, 259 F. Supp. 2d at 457. The court stated that foreign registrants using the <.org> TLD "chose, in effect, to play Internet ball in American cyberspace. Had they wished to avoid an American ACPA suit and transfer order and American jurisdiction altogether, they might have chosen to register the infringing domain name in top-level domains with solely foreign registries and registrars." *Id.*

²⁹⁸ The *Restatement of Foreign Relations Law* observes:

[C]omity has been variously conceived and defined. A well-known definition is: "Comity, in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons who are under the protection of its laws."

Supra note 19, § 101 cmt. e (citing *Hilton v. Guyot*, 159 U.S. 113, 163–64 (1895)); see also *RESTATEMENT OF FOREIGN RELATIONS LAW*, *supra* note 19, § 403 cmt. a.

²⁹⁹ See *Guyot*, 159 U.S. at 164 ("[Comity] is the *recognition* which one nation allows within its territory to the legislative, executive or judicial acts of another nation . . .") (emphasis added).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 85

claim, at least until a judgment is reached in one action.”³⁰⁰ The practice of extending comity, however, is generally accepted whenever the foreign court has proper jurisdiction and enforcement does not prejudice the rights of U.S. citizens or violate U.S. public policy.³⁰¹ Courts applying the ACPA in the context of international domain name disputes often recognize the need for comity analysis in decisions influencing other sovereigns’ legal interests—in particular, when the in rem provision was put into action.³⁰² U.S. courts generally do not consider comity principles a serious obstacle when applying the ACPA in international domain name disputes, however.³⁰³

One court evaluating the international implication of applying the in rem provision provided a relatively elaborate comity discussion. In *GlobalSantaFe Corp. v. GlobalSantafe.com*, the District Court for the Eastern District of Virginia considered whether it should defer to a previously issued injunction issued by a Korean court regarding a domain name.³⁰⁴ The court discussed at length the “Princess Lida” doctrine,³⁰⁵ which provides that in certain types of in rem actions, the first federal court to assert jurisdiction excludes other courts’ adjudication.³⁰⁶ Since the

³⁰⁰ *Laker Airways, Ltd. v. Sabena, Belgian World Airlines*, 731 F.2d 909, 939 (D.C. Cir. 1984).

³⁰¹ *V’Soske, Inc. v. Vsoske.com*, No. 00 Civ. 6099, 2003 U.S. Dist. LEXIS 5025, at *19 (S.D.N.Y. Apr. 1, 2003) (citing several Second Circuit authorities).

³⁰² *V’Soske*, 2003 U.S. Dist. LEXIS 5025, at *19.

³⁰³ *See, e.g., CNN Appeal*, No. 02-1112, 2003 WL 152846 (4th Cir. Jan. 23, 2003), (affirming lower court’s finding of jurisdiction without mentioning international comity concerns); *Mattel, Inc. v. Barbie-Club.com*, 310 F.3d 293, 302–03 (2d Cir. 2002) (indicating, in dicta, that international comity is not offended by the in rem ACPA provision, since Congress identified the U.S. registrar or registry of the domain name as the nexus to the U.S. jurisdiction) (citing H.R. REP. No. 106-412, at 14 (1999)); *Am. Online, Inc., v. AOL.org*, 259 F. Supp. 2d 449, 455–57 (E.D. Va. 2003) (concluding that international comity does not bar an injunction directed at the <.org> registry to transfer a domain name when the foreign registrar refuses to cooperate with the court); *GlobalSantaFe Corp. v. GlobalSantaFe.com*, 250 F. Supp. 2d 610, 626 (E.D. Va. 2003) (determining that U.S. federal court was not restricted by a prior foreign court order on the same domain name since the court in Virginia was first to assert jurisdiction, and since public policy and overriding U.S. interests justify such result).

³⁰⁴ *GlobalSantaFe*, 250 F. Supp. 2d at 617–26.

³⁰⁵ *Id.* at 624–25.

³⁰⁶ *Id.* (citing *SEC v. Banner Fund Int’l*, 211 F.3d 602, 611 (D.C. Cir. 2000); *Al-Abood v. El-Shamari*, 217 F.3d 225, 231 (4th Cir. 2000); *Princess Lida of Thurn & Taxis v.*

GlobalSantaFe court found that it was first in time to assert jurisdiction, it was “not obligated under the rule in *Princess Lida* to cede jurisdiction over the domain name in light of the subsequent order issued by the Korean court.”³⁰⁷ The *GlobalSantaFe* court further concluded that comity did not bar the application of the first-in-time rule under the circumstances.³⁰⁸

The application of a first-in-time rule in the context of the ACPA in rem provision raises the concern of a consequent “litigation race” situation, in which parties are encouraged to file suit before their opponent does. For example, as soon as the cloud of forthcoming dispute between a U.S. mark owner and a foreign registrant emerges, and where application of the in rem provision is in the vicinity, parties improve their position in a subsequent, indeed inevitable, court litigation, if they are the first to file an action in a court sitting in their preferred jurisdiction.³⁰⁹ Such a race may provide a negative incentive for parties considering whether to turn first to alternative dispute resolution methods. If international comity and the first-in-time rule are taken seriously enough to influence litigation strategies, international parties are more likely to elect court litigation and are likely to choose it earlier.

4. The ACPA Laundry Machine Effect and Its Paradox

The problems discussed above regarding application of the ACPA in international domain name disputes were especially pertinent to the in rem provision. U.S. courts did not consider those problems as a bar to their application of the ACPA in

Thompson, 305 U.S. 456, 465–66 (1939)). Although originally developed in the context of federalism, this doctrine has since been applied to federal cases with parallel proceedings underway in another country. *Id.* at 625 (citing *Banner Fund*, 211 F.3d at 611; *Dailey v. Nat'l Hockey League*, 987 F.2d 172, 175–76 (3d Cir. 1993)).

³⁰⁷ *GlobalSantaFe*, 250 F. Supp. 2d at 625.

³⁰⁸ *See id.* at 626 (finding that (i) U.S. and Korean proceedings were not concurrent; (ii) the Korean court proceeding was intended to frustrate the enforcement of a subsequent order of the U.S. court; (iii) enforcing the U.S. judgment is supported by significant U.S. public policy interests).

³⁰⁹ Such “litigation race” scenario contemplates a potential in rem action in the United States filed by the mark owner against some type of declaratory judgment action filed by the actual registrant in a foreign country, attempting to establish his or her rights in using the domain name.

difficult cases. Some commentators have raised serious concerns regarding this trend, however. They have argued that the in rem provision, as applied, is unconstitutional as violating due process,³¹⁰ that the extraterritorial reach of the ACPA is unreasonable under principles of international law prescriptive jurisdiction,³¹¹ that certain applications of the ACPA raise troubling questions concerning the overreaching of U.S. courts,³¹² and that the ACPA violates comity principles.³¹³ Without the need to address the merits of those assertions, this Article introduces another troubling aspect of the ACPA—its RDNH provision. The *Sallen* court teaches that any mark, U.S. or foreign, may be subject to the RDNH provision once a UDRP losing registrant exercises it.³¹⁴ The *Barcelona.com* court, however, teaches that only owners of U.S. marks may successfully defend the domain names in a RDNH action in U.S. courts.³¹⁵ In such cases, the ACPA becomes a clearinghouse, or a laundry machine, of foreign trademark rights in domain name disputes. Considering that the vast majority of UDRP challenges are commenced in U.S. courts,³¹⁶ this is a serious problem indeed. Such a result is likely to encourage forum shopping in international domain name disputes, a trend that is already facilitated by the UDRP Rules.³¹⁷

In some respects, the RDNH laundry machine effect is much more problematic than the in rem provision. In order to succeed in an in rem action, the plaintiff-mark-owner electing to sue in the United States must first establish the likelihood of confusion or

³¹⁰ Struve & Wagner, *supra* note 11, at 1006–18 (analyzing *Shaffer* as referring to all types of in rem jurisdictions and concluding that the ACPA in rem provision, lacking the requirement of minimum contacts, is unconstitutional).

³¹¹ Nguyen, *supra* note 288, at 552.

³¹² Bhanu K. Sadasivan, *Jurisprudence Under the In Rem Provision of the Anticybersquatting Consumer Protection Act*, 18 BERKELEY TECH. L.J. 237, 255 (2003).

³¹³ See Steven J. Coran, Note, *The Anticybersquatting Consumer Protection Act's In Rem Provision: Making American Trademark Law the Law of the Internet?*, 30 HOFSTRA L. REV. 169, 194–95 (2001).

³¹⁴ See *supra* Part II.B.3 (discussing the *Sallen* ruling).

³¹⁵ See *supra* Part III.B.2 (discussing the Fourth Circuit's *Barcelona.com* ruling).

³¹⁶ Efroni, *supra* note 24, at 367 & n.200 (finding that until late 2002 more than ninety-four percent of all court challenged UDRP decisions were commenced in the United States).

³¹⁷ See *supra* Part II.A.2 (discussing UDRP rule 3(xiii)(b)).

dilution and that the domain name was used in U.S. commerce.³¹⁸ Conversely, a registrant suing a foreign mark owner in a U.S. court under the RDNH provision must only show (1) registration; (2) suspension, disablement, or transfer of the registration in accordance with dispute resolution policy; (3) notice; and (4) that the plaintiff's registration or use of the domain name is not unlawful under the Lanham Act.³¹⁹ This burden of proof is light, especially if the owner is trying to avoid application of the Lanham Act by asserting no use in U.S. commerce at all.³²⁰ By definition, foreign marks are generally not protected by the Lanham Act; thus, owners of foreign marks have no defense but to try to assert U.S. trademark rights through use in U.S. commerce.

This Article takes the above assertion one step further: the laundry machine effect is inevitable, hopelessly rooted in the ACPA as a statute that regulates international cybersquatting disputes according to domestic trademark law. For example, the defendant, a foreign mark owner, challenged the court's subject matter jurisdiction in the *Sallen* case, arguing that the RDNH provision applied only to U.S. registered marks.³²¹ The court, in turn, correctly pointed out that such reading of the statute would bring about absurd results, leaving registrants unprotected against reverse domain name hijackers so long as the hijackers are not registered with the U.S. Patent and Trademark Office.³²²

Thus, out of the two possible alternatives, the court chose the only one that is logically and reasonably acceptable. In the *Barcelona.com* case, the court was asked to ascertain the scope of the RDNH provision, namely under which circumstances a losing registrant is protected under this provision.³²³ Again, the court

³¹⁸ See *supra* note 235 (noting that in order to succeed in an in rem action, plaintiff must establish infringement or dilution claims in accordance with regular Lanham Act requirements).

³¹⁹ See *supra* Part III.B.3 (discussing the *Barcelona.com* court's interpretation of the RDNH provision).

³²⁰ See *supra* note 260 and accompanying text (noting that this was exactly the theory of the city council in the *Barcelona.com* case and a prominent reason for its failure to obtain the domain name).

³²¹ *Sallen v. Corinthians Licenciamentos LTDA*, 273 F.3d 14, 23 (1st Cir. 2001).

³²² *Id.* at 25; see also *supra* text accompanying notes 173–79.

³²³ *Barcelona.com*, 330 F.3d 617, 623–29 (4th Cir. 2003).

faced two possible, alternative readings—registration must not violate *only* the Lanham Act, or, it must not violate *any* relevant trademark law involved. And again, the court upheld the reading that is not only compatible with the plain language of the ACPA and with trademark territoriality principles, but also the only logically and reasonably acceptable alternative.³²⁴ As mentioned earlier, the opposite reading would mean that under the ACPA, U.S. courts adjudicating RDNH actions should determine trademark rights protected by any possible relevant jurisdiction.³²⁵

Unfortunately, the *Sallen* and the *Barcelona.com* decisions remain logical and reasonable only when they stand alone. The combination of the two results in the above-mentioned laundry machine effect. Even under the assumption that the RDNH provision requires meeting U.S. constitutional personal jurisdiction tests,³²⁶ and even underestimating the effect of the UDRP Rules in helping registrants to establish such jurisdiction, the result for the owners of foreign marks is still very harsh. Considering the arguable expansion of U.S. personal jurisdiction rules in the digital age,³²⁷ the result may be not only harsh but also probable. It should be difficult to justify such a system as meeting the standard of “traditional notions of fair play and substantial justice.”³²⁸

E. Possible Foreign Reactions

In the “White Paper,”³²⁹ a statement of policy published by the National Telecommunications and Information Administration (“NTIA”), the U.S. executive branch explicitly recognized the need for international cooperation in regulating and controlling the

³²⁴ See *supra* Part III.B.2 (discussing the *Barcelona.com* holding and the court’s determination that Spanish law is inapplicable).

³²⁵ See *supra* Part IV.A (analyzing the *Barcelona.com* holding).

³²⁶ See *supra* text accompanying notes 178–83 (arguing that this question is still rather open).

³²⁷ See *supra* Part I.B.1 (discussing in personam jurisdiction).

³²⁸ See *Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (citing *Milliken v. Meyer*, 311 U.S. 457, 463 (1940)).

³²⁹ Management of Internet Names and Addresses, Statement of Policy, 63 Fed. Reg. 31,741, 31,746 (June 10, 1998) [hereinafter White Paper].

DNS.³³⁰ The ACPA, however, is an example of a combined U.S. legislative and the U.S. judiciary activism, which leads to a *de facto*, unilateral Internet regulation. Such activism might be conceived as an intimidating message sent to other Internet nations, with implications that go far beyond private domain name disputes.

It is reasonable to assume that U.S. treatment of international domain name disputes may invoke a strong reaction among foreign countries. One possible development could be that other sovereigns would enact their own anticybersquatting legislation.³³¹ The second possible development hypothesized by commentators was the scenario of “segmentation” of the Internet, as a result of a power struggle between America and other sovereigns.³³² Under

³³⁰ For example, in paragraph 11 thereof, the White Paper states: “The U.S. Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses [a function that now ICANN fulfills], a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet’s technical management.” White Papers, *supra* note 329. This aspect of the U.S. approach was sometimes called the “hands off” policy, assuring no direct, unilateral/governmental regulation of the DNS, at least not in the technical sense.

³³¹ At least in Japan, this is no longer mere possibility. The recently amended Unfair Competition Prevention Law (“UCPL”) provides in article 2(1)(xii) a new anticybersquatting cause of action. See Brent Yonehara, *LANDOFOTHERISINGSUN.CO.JP: A Review of Japan’s Protection of Domain Names Against Cybersquatting*, 43 *IDEA* 207, 221–24 (2003). The amended UCPL defines as actionable unfair competition “[t]he act of acquiring rights or preserving the right to use a domain name that is identical or similar to the indication of another person’s particular product (i.e., the name, trade name, trademark mark or other indication of goods or services of another person’s) for the purpose of gaining unfair profits or causing harm to another.” *Id.* at 221–22; see also Yamasaki Law Office, *New Developments in Japanese Law: Trademark Issues on the Internet in Japan*, at http://www.yamasaki-law.com/practice_5.htm#r5 (Aug. 30, 2001) (describing purpose of the Amendment).

³³² See Struve & Wagner, *supra* note 11, at 1032–34. Describing the phenomenon of segmentation, the authors state:

Segmentation arises when the various root server systems in use are either in conflict, or do not accurately reflect the content of other root servers . . . resulting in, for example, a request for www.yahoo.com yielding a different web page in different networks . . .

We predict that segmentation would result under the following circumstances:

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 91

this scenario, countries with enough resources, expertise, technology, and motivation would create a parallel Internet infrastructure with an alternative, competing domain name system.³³³ If and when such a development occurs, it is likely to result in a considerable reduction of benefits to Internet users, and probably a radical change in the status of the Internet as a prime source of information.³³⁴ These two possible types of reactions are likely to bring more harm than good, both to the United States and other Internet nations. The apprehension and frustration felt by other countries as a result of the current situation are indeed very real, and are likely to grow as U.S. interference with foreign trademark rights intensifies.³³⁵

V. A PROPOSAL FOR A BETTER MODEL: THE INTERNATIONAL ANTICYBERSQUATTING TREATY

This part consists of four sections. Section A highlights the problems of a unilateral approach to cybersquatting regulation and adjudication such as the one manifested in the ACPA. Section B presents a detailed alternative, a multilateral approach manifested in an international cybersquatting treaty scheme (“IACT”), which is based on ten fundamental principles. Section C tests the

First, a new root server system . . . could create conflicts with the existing public root server system

Second, and perhaps even more importantly, segmentation must be considered a potential response by one or more sovereigns to any others’ attempts to exert unwanted regulatory influence over the domain name system

. . . .

As should be easily apparent, segmentation of the domain name system would dramatically decrease its value to the Internet user community.

Id. (footnotes omitted).

³³³ *See id.*

³³⁴ *Id.* at 1034. One possible consequence of such segmentation is that it would no longer be possible to universally rely on any Uniform Resource Locator (“URL”) as a source of reference, since the same Internet address might randomly yield different results. *See id.*

³³⁵ *See* Christopher P. Rains, Comment, *A Domain by Any Other Name: Forging International Solutions for the Governance of Internet Domain Names*, 14 EMORY INT’L L. REV. 355, 371 (2000) (noting the implications of imposing a single’s nation law on all Internet-faring nations go largely unnoticed among U.S. policymakers and how the frustration felt by foreign plaintiffs—and indeed foreign courts—is very real).

proposed model using two methods; first it applies the *Barcelona.com* dispute in a world governed by the proposed IACT, examines the expected outcome, and compares it with the actual outcome in that case. Second, it provides a more general game-theory model that proves the assertions of forum shopping motivation and the advantages of the new scheme over the present one. Section D argues that the proposed model should be attractive and advantageous both to the United States and other Internet nations. While doing so, it examines some possible weaknesses of the proposed model and offers some answers.

A. Unilateral Approach: A Lose-Lose Situation

If other nations react to the United States' current policy by enacting their own domestic cybersquatting laws, the situation may only get worse. A growth in the number of conflicting decisions regarding the same dispute in different national courts would have grave consequences on legal certainty, fairness, and international comity, and thus should be strongly discouraged.³³⁶ In addition, it is questionable whether such laws would have a significant effect on disputes that arguably involve U.S. public policy interests.³³⁷ As noted earlier, U.S. courts have already demonstrated an aggressive enforcement approach, ordering registries and a registrar to effectuate their decisions.³³⁸ The fact that the registries of all major, unrestricted gTLDs are located on U.S. soil³³⁹ makes

³³⁶ After the anti-cybersquatting bill passed the House of Representatives, Clinton White House spokesman Joe Lockhart stated, "We believe that fundamentally we'd be walking down the wrong road if we legislated a cybersquatting law and then the 200 or so Internet countries around the world started legislating their own rules and laws." Statement by Joe Lockhart, White House Press Secretary (Oct. 28, 1999), *noted in* Springer, *supra* note 8, at 359 & n.281.

³³⁷ See, e.g., *V'Soske, Inc. v. V'soske.com*, No. 00 Civ. 6099, 2003 U.S. Dist. LEXIS 5025, at *19 (S.D.N.Y. Apr. 1, 2003) (concluding that even when another foreign court may properly assert jurisdiction over a dispute, it does not prejudice the rights of U.S. citizens or violate domestic public policy).

³³⁸ See *CNN II*, 177 F. Supp. 2d 506 (E.D. Va. 2001); see also *supra* note 295 and accompanying text (describing recent U.S. case law finding overriding U.S. interests in applying the ACPA to international disputes); *supra* notes 152-53 and accompanying text (describing U.S. courts' enforcement measures against registration authorities in order to give effect to their rulings).

³³⁹ See *supra* note 15 and accompanying text.

a conflicting foreign legal process in many cases unenforceable, and indeed, meaningless.³⁴⁰ Put differently, a U.S. injunction against the gTLD registry has proven to be stronger than any conflicting foreign law or judicial order.³⁴¹ Indeed, since physical control over Internet infrastructure *does* matter,³⁴² U.S. courts are potentially the final arbiters in many cybersquatting disputes.³⁴³

Moreover, it is likely that legislation of foreign anticybersquatting laws regulating gTLD registrations, if and when it comes,³⁴⁴ would be as problematic as the ACPA and suffer from similar symptoms. These laws would probably afford effective protection to marks recognized by the relevant national trademark law, and at the same time, afford little, if any, protection to cybersquatted marks that the national law does not protect. Such a result occurred in the case of the ACPA as applied in the

³⁴⁰ See *GlobalSanteFe Corp. v. GlobalSantaFe.com*, 250 F. Supp. 2d 610, 626–27 (E.D. Va. 2003) (issuing an injunction against the <.com> registry to enforce its judgment and disable the domain name until it is transferred to the mark owner, despite a Korean court’s order telling the Korean registrar not to do so); see also *Am. Online, Inc. v. Aol.org*, 259 F. Supp. 2d 449, 457 (E.D. Va. 2003) (issuing an injunction against the <.org> registry to enforce the transfer of the domain name to the mark owner when the foreign registrar refused to cooperate with the court).

³⁴¹ *Id.*

³⁴² Struve & Wagner, *supra* note 11 at 992–93. The authors observe that the regulatory authority of a sovereign with the principal infrastructure of the domain name system located in its territory “can be grounded in either the widely-accepted principles of prescriptive jurisdiction or the de facto result of the physical location of elements of the domain name system.” *Id.* at 992. The authors continue:

In the prescriptive jurisdiction case, the location of certain elements, specifically the root or TLD servers, within a sovereign’s territory will in almost all cases provide at least substantial international legal support for the assertion of jurisdiction . . . de facto control can be exerted via the reality of the technology and geography. In either event, the same basic point holds: geography matters.

Id. at 992–93 (footnote omitted). In these contexts, geography matters not only as a prescriptive jurisdiction element, but also regarding jurisdiction to enforce. See *supra* note 21.

³⁴³ Nguyen, *supra* note 288, at 535–40 (warning against the formation of an in rem court by default in the Eastern District of Virginia, resulting from the fact that major gTLD registries are located there).

³⁴⁴ For example, see *supra* note 331 (noting the new Japanese anticybersquatting provision). Japan’s law probably protects against cybersquatting in gTLDs in addition to <.jp> domains, albeit protection is based on different principles than in the United States. See Yonehara, *supra* note 331, at 221–24 (2003) (describing Japan’s protection against cybersquatting and comparing it to the ACPA).

Barcelona.com ruling, and such a result should be avoided instead of replicated.

An interesting question is whether foreign mark owners should take the advice offered by the Eastern District of Virginia. In two recent decisions, this court used language that suggested ccTLD registrations enjoyed ACPA immunity.³⁴⁵ Further, ccTLD registrations are not subject to the compulsory UDRP, unless voluntarily adopting it.³⁴⁶ Can ccTLD registrations solve the problem of international domain name disputes? Probably not.³⁴⁷ The fact that ccTLD registries are subject to regulation and control of the corresponding national governments is a matter of mere U.S. government courtesy.³⁴⁸ There is no guarantee against the following scenario: one day, the U.S. Department of Commerce concludes that certain ccTLD registrations are posing serious threats to U.S. interests. Therefore, ICANN is delegated the responsibility to make sure that U.S. interests, including trademark rights, are not infringed through such registrations.³⁴⁹ Though it could be argued that such a scenario is very unlikely, it is still technically possible. A careful reading of some of recent U.S. court decisions may be regarded as an implied call by the courts for putting order in the unruly ccTLD system.³⁵⁰ More importantly, in the context of the RDNH provision, this solution is

³⁴⁵ See *supra* note 296–97 and accompanying text.

³⁴⁶ Sharrock, *supra* note 17, at 841–42 (noting that ccTLD registrars are not required to bind their registrants to the UDRP, although country code registration authorities can voluntarily adopt the policy).

³⁴⁷ This issue may require a more comprehensive discussion. The Article, however, only touches upon some arguments indicating that ccTLD registrations as a comprehensive solution is inadequate.

³⁴⁸ See von Arx & Hagen, *supra* note 4, ¶ 20. The authors observe:

Technically, the ccTLDs are subdomains of the “root domain” created by the U.S. government and “contained” in the root zone file. Despite the U.S. reservation of technical control over the A root, the U.S. government states that “[n]ational governments now have, and will continue to have, authority to manage or establish policy for their own ccTLDs,” thereby attempting to downplay the influence that the U.S. may indirectly have over the policies of nations foreign to the U.S.

Id. (footnote omitted).

³⁴⁹ See *id.* The U.S. control over the A root server provides the power to create, redelegate, or destroy ccTLDs. See *id.* ¶ 2.

³⁵⁰ See *supra* note 296.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 95

meaningless. Foreign mark owners never chose gTLD registrations in such cases—the registrant did. In fact, the foreign owner may have neither gTLD nor ccTLD registrations, yet still be forced to submit to ACPA rules in U.S. courts.

B. Possible Solution: The IACT

The discussion thus far suggests that the evil is rooted in the national/unilateral approach to cybersquatting regulation and adjudication. The first clear example for the inadequacy of this approach is, of course, the ACPA itself. The IACT offers an alternative. A draft of the IACT would be prepared by an international organization with recognized specialty, experience, and reputation, such as WIPO. Such a treaty shall be signed by all nations wishing to become “member states” and willing to adhere to its principles. The important IACT fundamentals are summarized by the following ten principles:

- (1) Domestic Legislation: All member states must legislate within a certain timeframe domestic anticybersquatting laws protecting against abusive registrations of domain names incorporating trademarks.³⁵¹ The heart of this legislation would be a cybersquatting standard that must not be lower than the “minimum standard” stipulated in the IACT.³⁵² This law should also include a RDNH provision, protecting registrants against unjustified claims, an in rem

³⁵¹ An example of implementing international intellectual property standards through domestic legislation by member-states can be found in articles 44–49 of the Agreement on Trade-Related Aspects of Intellectual Property Rights. See Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Apr. 15, 1994, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 1 (1994), 33 I.L.M. 1125 (1994); Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization [hereinafter WTO Agreement], Annex 1C, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 31, 33 I.L.M. 81 (1994) [hereinafter TRIPS Agreement]. For congressional approval of the TRIPS and WTO Agreements, see Uruguay Round Agreements Act, Pub. L. No. 103-465, 101-103, 108 Stat. 4809, 4814-19 (1994) (codified in scattered sections of 15, 17, 19, and 35 U.S.C.). See also J.H. Reichman, Comment, *Enforcing the Enforcement Procedures of the TRIPS Agreement*, 37 VA. J. INT'L L. 335, 340–41 (1997) (describing the relevant implementation and enforcement articles of the TRIPS Agreement).

³⁵² See *infra* text accompanying note 355 (discussing principle 2).

provision,³⁵³ and other essential features of effective anticybersquatting legislation.³⁵⁴

(2) Minimum Standard: The IACT shall stipulate an agreed-upon minimum standard for unlawful cybersquatting. A member state should be allowed, if it deems appropriate, to incorporate a higher standard in its domestic legislation (i.e., a wider range of Internet activities would fall under the definition of unlawful cybersquatting). No standard lower than the IACT minimum standard shall be permitted, however.³⁵⁵

(3) Mutual Protection: All member states should be obliged to protect against cybersquatting marks recognized and protected by any other member state. In a cybersquatting dispute involving a mark protected under the other member state's law, a member state generally should adjudicate the cybersquatting dispute in accordance with its own domestic anticybersquatting norms, and under the assumption that the mark is valid and protectable.

(4) Judicial Assistance: In order to determine whether there is a protected foreign mark, or "IACT mark," involved, member states shall create a system of "judicial assistance."

³⁵³ A recommended in rem provision should establish jurisdiction only in cases in which the registrant cannot be found or identified. Due to the conceptually elastic of interpretation of where exactly the physical location of a domain name is, making it eligible for in rem actions, contracting member states may reach an acceptable definition of the appropriate adjudicating forum in those instances. In any event, as suggested in principle 10, the International Anticybersquatting Treaty ("IACT") generally provides personal jurisdiction when the opponent is identified and connected to some other member state. This provision should cover the vast majority of disputes in the first place.

³⁵⁴ The assumption is that member states have already at least minimal trademark protection in place, and that such states adhere to universally accepted concepts of fair judicial process and commitment to the rule of law.

³⁵⁵ A prominent example of such an attempt to ascertain internationally accepted minimum standard against cybersquatting was demonstrated in WIPO's final report to ICANN, in the spirit of which the UDRP was crafted. See WIPO, FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS ¶¶ 170–77 (1999) (defining abusive registration) [hereinafter WIPO FINAL REPORT], available at <http://wipo2.wipo.int/process1/report/finalreport.html> (last visited Nov. 5, 2003). But see Helfer & Dinwoodie, *supra* note 101, at 168–70 (questioning the authority and legitimacy of WIPO to create the standards embodied in the final report).

In a situation described in principle 3 above and in any other instance where foreign trademark rights should be ascertained, the “adjudicating court,” or the court where the complaint is filed, would submit a query to a proper court in the jurisdiction where the mark arguably is protected, the “assisting court.” The query shall be in a standard format and limited in scope. It should ask the assisting court one question, and one question only: whether the arguably cybersquatted mark is protected by law in the assisting court’s jurisdiction.

(5) Determination of IACT Mark: A final judicial determination of the assisting court shall be decisive on the matter of whether the mark constitutes an IACT mark and whether it falls within the scope of the IACT’s authority.³⁵⁶

(6) Choice of Law I: If (i) a plaintiff-mark-owner files an IACT action in a court in a member state different from the member state under which law the mark is arguably protected, as opposed to the “state of origin” (i.e., where the mark is protected); and (ii) the standard for cybersquatting protection in the adjudicating court is *higher* than the standard in the state of origin, then the *lower* standard of the two should be applied.³⁵⁷

³⁵⁶ A possible appeal procedure may also be considered in this context. Under such a procedure, the aggrieved party would be able to appeal to a higher court in the assisting court’s jurisdiction. In such a case, the final judicial finding in that jurisdiction would be decisive.

³⁵⁷ Here, a mark owner is choosing a forum that does not protect the mark in its domestic legislation. Such a rule is important to prevent forum shopping of mark owners, suing in the member state with the highest standard of protection. In case that a mark is arguably protected in more than one member state, two situations should be regulated: (1) the mark is arguably protected both in the adjudication court and in other member states; (2) the mark is arguably protected only in some other multiple member states. In the former situation, the better rule is that the adjudication court’s standard would apply (even in a case in which the standards in the other jurisdictions are lower). The rationale is to allow a mark owner who files an action in a jurisdiction where the mark is protected to enjoy the domestic cybersquatting protection standard. In the latter situation, the lowest standard involved should be compared with the adjudication court’s standard, and the lower between the two should be applied. The aim here is to discourage a mark owner from filing an action in a jurisdiction where the mark is not protected in an attempt to benefit from its higher protection standard.

(7) Choice of Law II: If (i) a plaintiff-registrant who lost a domain name registration in a UDRP or other similar proceeding brings an RDNH complaint in an adjudicating court residing in a jurisdiction different from the state of origin; and (ii) the standard of the adjudicating court is *lower* than the standard of the state of origin, then the *higher* standard of protection should apply.³⁵⁸

(8) Choice of Law III: Regarding the factual determination of which standard is higher and which standard should be applied in a specific case, the adjudicating court shall have sole discretion.³⁵⁹

(9) First in Time, First in Right: If the adjudicating court determines that both parties have cognizant rights in the mark under any of the trademark laws involved (i.e., both have a protected IACT mark), then “first in time, first in right” rule should apply.³⁶⁰ If only one party establishes rights in an IACT mark, however, the adjudication court shall render the appropriate judgment securing that party’s rights in the corresponding domain name.³⁶¹

(10) Uniform Personal Jurisdiction Rule: The domestic legislation should also include a special uniform personal jurisdiction rule. This rule should generally provide an adjudicating court with personal jurisdiction over a

³⁵⁸ The same rationales and considerations discussed in principle 6 also are relevant in this situation, with necessary adjustments. *See supra* note 357 and accompanying text. This rule encourages filing of RDNH actions in jurisdiction(s) where the mark is a protected, as opposed to the *Barcelona.com* situation. Conversely, if registrants wish to avoid litigation in a foreign country (in cases where the protecting jurisdictions are different than their country of residence), the door is still open to file the action anywhere else subject to principle 10, but they compromise for a higher standard of cybersquatting protection.

³⁵⁹ One might suggest the establishment of an appellate panel comprised of international experts, to which an aggrieved party may appeal *only* on this issue of applicable cybersquatting standard under the IACT rules.

³⁶⁰ Namely, the registrant gets to keep the domain name registration. .

³⁶¹ In order to enforce the adjudicating court’s decision *vis-à-vis* registration authorities, it seems that close cooperation with ICANN would be necessary. In addition, an ancillary rule of *res judicata* should be installed, giving the adjudicating court’s decision a binding power in any of the other member state

defendant (either a mark owner or registrant) in a domain name dispute filed under the IACT. A defendant in such an IACT complaint filed in a proper venue in one of the member states shall be barred from bringing a personal jurisdiction objection.³⁶²

In sum, the idea of the IACT is rather simple: the IACT creates a new legal and conceptual creature: the IACT mark. Such mark would be a protected *trademark* under at least one member state's law, but protected against *cybersquatting* in all member state jurisdictions.³⁶³

³⁶² A proliferated "proper venue" rule should be articulated in the IACT. A proposed rule could be the following four-level priority scheme: (1) if the jurisdiction where the mark is protected and where defendant is a resident (or where personal jurisdiction can be otherwise obtained according to the regular domestic rules) is the same jurisdiction, then plaintiff should sue there; (2) if these jurisdictions are different, then plaintiff should sue where the defendant resides (or where personal jurisdiction is otherwise available), unless plaintiff is able to establish minimum contacts of defendant with the member state where the mark is protected, upon such case plaintiff may alternatively sue there (the test may be based on the U.S. minimum contacts concept or a similar one); (3) if neither of the above two rules apply, then plaintiff should sue where minimum contacts of the defendant with the member state's jurisdiction exist; (4) if plaintiff sues in a member state where defendant is not a resident (and personal jurisdiction is not available), where the mark is not protected, and where minimum contacts do not exist, then that member state should nevertheless adjudicate the dispute upon a satisfactory explanation of the reason for suing there and upon determination that the venue was not chosen in bad faith. When plaintiff follows this rule, principle 10 should secure personal jurisdiction. In the appropriate cases, courts may use the *forum non conveniens* doctrine in order to transfer suits to a more suitable forum.

³⁶³ In a recent article, Professor Rochelle C. Dreyfuss and Professor Jane C. Ginsburg presented a detailed proposal for a draft of convention on intellectual property matters ("Draft"). See *Draft Convention on Jurisdiction and Recognition of Judgments in Intellectual Property Matters*, 77 CHI.—KENT L. REV. 1065 (2002). That proposal for an international convention was specifically intended to include also domain name disputes. *Id.* at 1074 (the text of article 1 of the Draft specifically includes "claims involving domain names."). The jurisdictional and adjudication solutions presented in the draft, however, are significantly different from the solution proposed by the IACT. First, the Draft is intended also to cover myriad of intellectual property matters such as copyrights, neighboring rights, trademarks, unfair competition, and more. See *id.* Second, the Draft is intended to cover disputes regarding violations occurring not only on the Internet but also in the off-line world. See *id.* The Draft contains no language that restricts its scope only to on-line infringements. Therefore, an instrument such as the IACT mark of which protection is limited only in the domain-names-incorporating-trademarks context would be inapplicable.

C. Testing the Model

1. Applying *Barcelona.com* in an IACT Legal Framework

After introducing the model, the Article now turns to examine what result in the *Barcelona.com* case would have been in an IACT world. Assume that both the United States and Spain are member states of the hypothetical IACT. Assume further that both legislated essentially similar anticybersquatting laws as mandated by the IACT. The City Council of Barcelona files and wins a UDRP proceeding, where it asserted its trademark rights under Spanish law in the term Barcelona. The registrants now seek reversal and contemplate where to file a RDNH complaint. If they sue in Spain, then the Spanish court would typically have to decide first whether the term Barcelona is a protected mark in Spain and whether the rights in the mark belong to the City Council. If the court rules in the affirmative in both questions, then the court should further apply the Spanish anticybersquatting law and determine whether the registration of the domain name violated that law.

Alternatively, the registrants may decide to sue in a U.S. court under the *modified* ACPA.³⁶⁴ According to the IACT definitions the U.S. court would be the adjudicating court, and the Spanish court would be the assisting court. First, the U.S. court should be able to have in personam jurisdiction over the City Council, in accordance with principle 10.³⁶⁵ After concluding that the term Barcelona is not protected under U.S. law,³⁶⁶ a query to the proper court in Spain should be submitted, where the Spanish trademark rights in the term shall be ascertained under Spanish law. If the Spanish court determines the existence of such rights, the U.S.

³⁶⁴ That is, an ACPA that is accommodated to comply with the IACT scheme described above.

³⁶⁵ See *supra* note 362 and accompanying text (discussing principle 10). Defendant (the city council) is not a U.S. resident, the mark is not protected there, and it is also possible that there are no minimum contacts between the city and the United States. Alternative 4, however, in the sliding scale described in *supra* note 362 may nevertheless provide jurisdiction, by virtue of the IACT agreement.

³⁶⁶ This conclusion is reached for the same reasons delineated in the actual *Barcelona.com* decision. See discussion *supra* Part III.B.4.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 101

court shall proceed to adjudicate the dispute according to the modified ACPA under the assumption that the mark is protected. If no such Spanish trademark rights are established, the registrants should keep the domain name without the need to further discuss cybersquatting allegations.

Consequently, the result should be identical, regardless of whether the registrants elect to sue in a U.S. or Spanish court.³⁶⁷ Thereby, the problems of forum shopping and the frustration felt by owners of foreign marks sued in the United States would be essentially eliminated. Even if some of the basic assumptions are changed—for instance, that the cybersquatting standards are different in Spain compared to those in the United States—the applicable law would still be the higher standard of cybersquatting.³⁶⁸ That means that losing registrants in the UDRP proceeding would no longer have a more attractive forum that would entertain their RDNH claim. Even in more internationally complex circumstances, the result would be essentially similar. The incentives to forum shop for the venue applying the most favorable law, both by registrants and mark owners, would dramatically decrease.³⁶⁹ Another advantage of this scheme is that a qualified Spanish court would decide on matters of Spanish trademark law, instead of a U.S. court in Virginia, struggling with Spanish trademark terminology, legal analysis and interpretation.³⁷⁰

³⁶⁷ Actually, it would not really matter whether registrants alternatively elect to sue in a third member state's court. Under the *Barcelona.com* circumstances, it would always be Spanish law determining the existence of the mark and the adjudicating court's cybersquatting standard applied, unless the circumstances call for application of the Spanish standard, where principal 7 is applicable.

³⁶⁸ See *supra* note 357.

³⁶⁹ A more complex hypothetical situation could be, for instance, a Korean registrant arguably cybersquatting on a Chinese mark using a Japanese registrar. Assuming that all three jurisdictions adhere to the IACT, the rights in the mark would be determined in the three possible adjudicating courts according to Chinese law under a cybersquatting standard least favorable to the plaintiff or the standard of the "state of origin" (in this case, China). If trademark rights of both parties can be established (e.g., the registrant has rights under the law of Japan and the mark owner established Chinese rights), then principle 9 applies; the registrant who was first to register his mark would be allowed to keep the domain name.

³⁷⁰ The district court in the *Barcelona.com* dispute put itself in the shoes of a Spanish court, discussed Spanish trademark law, and made judicial findings applying that law.

2. The Game Theory Model

Thus far, the Article contests that the ACPA RDNH provision unreasonably favors U.S. marks, namely, because only such marks have an effective defense against RDNH claims in U.S. courts. As a consequence, the Article envisions some negative effects, including forum shopping, where owners of foreign marks are motivated to avoid U.S. forum while registrants are strongly encouraged to file RDNH actions against such owners in U.S. courts.

The following numerical model examines the ACPA from a more general perspective, which is not limited to RDNH cases. While also scrutinizing the ACPA in light of its in personam and in rem provisions, the model attempts to show the general imbalanced structure of the ACPA, which facilitates a plaintiff-sensitive forum shopping situation.³⁷¹

In the aftermath of the *Sallen* and the *Barcelona.com* decisions, it appears that judicial outcomes in international cybersquatting disputes litigated in U.S. courts are becoming more predictable. Hence, under this model, numerical values are assigned to different world situations or scenarios.

There are two types of rational actors participating in any situation evaluated by the model: registrant (*R*) and mark owner (*MO*). Similar to other typical behavioral models, this model assumes that both actors aspire to maximize their utility and make informed decisions accordingly. In addition, this model contemplates three variables:

- (1) Venue: The two possible alternatives are either the United States or *Jurisdiction X*.

See Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona, 189 F. Supp. 2d 367, 371–72 (E.D. Va. 2002), *rev'd and vacated*, 330 F.3d 617 (4th Cir. 2002)

³⁷¹ Since registrants as plaintiffs will always attempt to bring RDNH actions, while owners as plaintiffs will exercise the in personam and in rem provisions, the general model also includes the RDNH problem.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 103

(2) Applicable Trademark Law: The two possible alternatives are either U.S. law or *Jurisdiction X* law.³⁷²

(3) Plaintiff: The two possible alternatives are (i) *R* filing a RDNH action after losing its registration in the UDRP (or through application of a similar policy);³⁷³ or (ii) *MO* filing a trademark infringement or dilution action.³⁷⁴

When the mark in question is likely to be protected in the venue's jurisdiction³⁷⁵ then the symbol (TM+) is assigned, as opposed to situations where the mark is not protected (TM-).

The model further assumes that a plaintiff suing in a certain venue would make three types of arguments: (1) the chosen venue has personal jurisdiction (*PJR*) over the defendant;³⁷⁶ (2) the chosen venue has subject matter jurisdiction (*SMJ*) to adjudicate

³⁷² Trademark law in this context includes both substantive trademark protection—that is, general definitions of protected marks and circumstances under which protection is triggered—and protection against cybersquatting.

³⁷³ For purposes of convenience, the model further refers only to the UDRP. The analysis, however, should apply also to any other policy falling under the RDNH provision of the ACPA.

³⁷⁴ Arguably, these are not the only possible world situations. For example, registrant (*R*) may try to secure a declaratory judgment through a “preemptive lawsuit” before mark owner (*MO*) takes any measures. The model argues, however, that this situation would be very rare. The first reason is the immediate, substantial litigation costs involved. Rational *R* would try to avoid litigation absent an imminent threat to the registration. Even if *MO* files a UDRP complaint, there is still hope that *R* would win the UDRP proceeding. Thus, it makes no sense for *R* to be impatient at this early stage. Second, such an action would prevent *R* from implementing litigation strategies, in the relevant situation, that would help *R* in directing subsequent judicial proceedings to *R*'s favorite jurisdiction. *R* filing a preemptive lawsuit is generally confined to a jurisdiction where personal jurisdiction over *MO* is available. Third, *R* filing a “preemptive lawsuit” is expected to have a significant cause of action problem. Even the *Sallen* holding is not directly applicable where a subsequent UDRP proceeding never took place. Fourth, being the first to bring a lawsuit does not seem to furnish *R* with a significant strategic advantage. *But see supra* Part IV.D.3 (discussing the *GlobalSantaFe* case and indicating that in some cases of possible in rem actions in the United States, it might be important for *R* to sue first in order to overcome comity problems). In sum, a “preemptive lawsuit” strategy in general is likely to be very unattractive for *R*, hence negligible for the purpose of the model.

³⁷⁵ This is the case, for example, when an official trademark registration exists and maintained by *MO*.

³⁷⁶ Since the model assumes international elements and interests involved in the dispute, it is likely that defendant would bring also a personal jurisdiction challenge.

the dispute;³⁷⁷ and; (3) plaintiff is entitled to the relief sought (*Merits*).³⁷⁸ In addition, the model assigns numerical values to each scenario: the value 1 is assigned when the plaintiff is likely to succeed in the argument, the value 0 is assigned when the plaintiff is likely not to succeed and the value 0.5 is assigned when the plaintiff may succeed. Utility value (*UV*) is the sum value in all three arguments in a certain situation, while the aggregate value of the *UV*s in any one of the venues is the total utility value (*TUV*) of a certain plaintiff litigating in a certain venue.

a) The Post-*Barcelona.com* World

Table A
R's Alternatives in a Post-*Barcelona.com* World

Situation	United States		<i>Jurisdiction X</i>	
	I	II	III	IV
<i>TM</i>	+	-	+	-
<i>PJR</i>	0.5* (1)	0.5 (1)	0.5 (1)	0.5 (1)
<i>SMJ</i>	1	1	0.5	0.5
<i>Merits</i>	0.5	1	0.5	0.5
<i>UV</i>	2 (2.5)	2.5 (3)	1.5 (2)	1.5 (2)
<i>TUV</i>	4.5 (5.5)		3 (4)	

* The value in parenthesis is the *PJR* value when plaintiff employs pre-litigation strategies.

³⁷⁷ That is, the venue acknowledges and renders appropriate recourse in cases of cybersquatting and/or RDNH claims.

³⁷⁸ The nature of the merits sought and its availability depends, naturally, on the applicable law. The precise remedies available for the plaintiff in the various situations is not a relevant parameter of the model and thus are not specified.

Table B
MO's Alternatives in a Post-Barcelona.com World

Situation	United States		<i>Jurisdiction X</i>	
	I	II	III	IV
<i>TM</i>	+	–	+	–
<i>PJR</i>	1	0.5	0.5	0.5
<i>SMJ</i>	1	0	0.5	0.5
<i>Merits</i>	0.5	0	0.5	0.5
<i>UV</i>	2.5	0.5	1.5	1.5
<i>TUV</i>	3		3	

i. Explanation

In situation I in table A, *R* is filing a complaint in a U.S. court under the RDNH provision of the ACPA after losing the registration in the UDRP. Situation I also provides that the mark in question is protected under the venue's law, i.e., the Lanham Act. Since foreign elements are involved, the model assumes that *MO* would bring *PJR* challenge, and the chances of *R*'s success in convincing a U.S. court to exercise *PJR* over *MO* are evaluated at 0.5. Further, since the RDNH provision of the ACPA renders a certain *SMJ* in such a case,³⁷⁹ the value assigned in the relevant field is 1. If *R* is successful in asserting personal and subject matter jurisdiction in the United States, and given that the mark is protected under the Lanham Act, *R* may or may not further succeed in showing that the registration does not violate the ACPA, hence the value 0.5 in the *Merits* field.

Situation II in table A differs from the previous scenario only with respect to the validity of the mark under U.S. law. It provides a scenario in which the mark is not protected under the Lanham Act. In light of the outcome in the *Barcelona.com*, the value 1 is assigned in the *Merits* field, and the probability for *R* to win in court is very high.

On the other hand, consider situation III in table A. Success in asserting *PJR* and *SMJ* in *Jurisdiction X* in a RDNH claim is

³⁷⁹ This example relies on a *Sallen* analysis.

questionable, hence the value 0.5 is assigned.³⁸⁰ Even if *R* is successful in both arguments, *R* may convince the court that the registration is not unlawful, even though the mark is protected under *Jurisdiction X* law. In situation IV in table A, where the mark is not protected under *Jurisdiction X* law, the value 0.5 is still assigned in the *Merits* field because the model cannot predict whether the foreign court would resolve to grant cybersquatting protection in an RDNH claim even to non-recognized marks.³⁸¹ Finally, the values in parentheses assigned across the *PJR* fields of table A indicate that *R* may also use litigation strategies in order to increase its chances to establish personal jurisdiction over *MO* in the chosen venue, as discussed in Part II.A.2 of this Article. Since “locking” *MO* in a certain jurisdiction dramatically increases *R*’s chances to establish *PJR*, the value 1 in parenthesis is assigned.

Table B presents the possible alternatives available for *MO* in a post-*Barcelona.com* world. In situation I, *MO* files a cybersquatting action against *R* in a U.S. court, where the mark is protected. *MO* has value 1 in the *PJR* field because the model assumes that lack of personal jurisdiction over *R* does not bar a cybersquatting action in the United States.³⁸² *MO* has value 1 also in the *SMJ* field³⁸³ and value 0.5 in the *Merits* field.³⁸⁴ In situation

³⁸⁰ Subject matter jurisdiction for losing registrants should not be taken for granted in any given jurisdiction. Some jurisdictions may consider the UDRP as arbitration and refuse to interfere (or, altogether refuse to acknowledge any cause of action providing redress to *R* in such circumstances). For instance, in the United States it took the legislation of the ACPA and the ruling of *Sallen* to establish such subject matter jurisdiction. In addition, one U.S. appellate court has held that the UDRP is not a proceeding falling under the Federal Arbitration Act. *See Dluhos v. Strasberg*, 321 F.3d 365, 371–73 (3d Cir. 2003) (concluding that the UDRP proceedings do not fall under the Federal Arbitration Act, thus the court was not limited to that act’s constraints on UDRP judicial review).

³⁸¹ The *Barcelona.com* district court believed that the ACPA affords such protection. *See* 189 F. Supp. 2d 367, 373–74 (E.D. Va. 2002), *rev’d and vacated*, 330 F.3d 617 (4th Cir. 2002).

³⁸² When personal jurisdiction in the United States cannot be ascertained, *MO* is likely to invoke the in rem provision. *See supra* Parts II.B.2, IV.D (providing discussions on the ACPA in rem provision and indicating that in rem jurisdiction is available when in personam jurisdiction cannot be established). Since the gTLD registries, by and large, are located in U.S. territory, *MO* using the in rem provision is very likely to succeed in establishing basis for jurisdiction in the United States.

³⁸³ This is provided by the ACPA. *See* 15 U.S.C. § 1125(d) (2000).

³⁸⁴ The result depends of *MO*’s ability to establish its ACPA claims.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 107

II in table B, *MO* is likely to be required by a U.S. court to establish personal jurisdiction over *R*, since the ACPA in rem provision is not available when a foreign mark is involved, hence the value 0.5.³⁸⁵ Further, the model assumes that the ACPA does not protect non-U.S. marks, therefore the value 0 appears in the *SMJ* field.³⁸⁶ Absent a U.S. recognized mark, and failing to establish *SMJ*, *MO* has practically zero chance to win the merits of a cybersquatting claim under the ACPA.³⁸⁷ Table B further presents *MO*'s values in *Jurisdiction X* according to the same principles.³⁸⁸ Tables A(a) and B(b) below presents the *UV* results of Tables A and B, respectively.

Table A(a)
R's UV in a Post-Barcelona.com World

		<i>Jurisdiction X</i>	
		+	-
United States	+	2 / 1.5	2 / 1.5
	-	2.5 / 1.5	2.5 / 1.5

Table B(b)
MO's UV in a Post-Barcelona.com World

		<i>Jurisdiction X</i>	
		+	-
United States	+	2.5 / 1.5	2.5 / 1.5
	-	0.5 / 1.5	0.5 / 1.5

³⁸⁵ See *supra* note 235 (indicating that the in rem provision covers only U.S. protected marks).

³⁸⁶ But see *supra* note 262 (discussing an alternative reading of the ACPA).

³⁸⁷ See *id.*

³⁸⁸ In situations III and IV in table B, territorial jurisdiction is always uncertain. Further, *MO* is assigned the value 0.5 in the *SMJ* fields, since it is questionable whether *Jurisdiction X* recognizes its cause of action absent of legislation similar to the ACPA and/or other legal bases providing cybersquatting protection. In situation IV in table B, *MO* holds no trademark rights under *Jurisdiction X* law. The model, however, cannot predict whether *Jurisdiction X* affords cybersquatting protection even when the mark is not recognized under its trademark system.

ii. Analysis

The results unequivocally affirm the basic assumption of a plaintiff-sensitive forum shopping situation. Table A shows that *R* has a significant positive incentive (+1.5) to litigate in the United States.³⁸⁹ In addition, table A(a) indicates that *R* has such motivation *regardless of the nature of trademark rights involved*.³⁹⁰ Table A further shows that *R*, implementing litigation strategy, is increasing his *TUV* in both the United States and *Jurisdiction X*.³⁹¹

Table B shows that *MO* is technically indifferent between litigating in the United States or in *Jurisdiction X*.³⁹² A closer look at table B(b), however, reveals that *MO*'s decision is highly dependent on the "nationality" of the mark. Table B(b) shows that *MO* is expected to favor the U.S. forum in two out of four possible situations—only when a U.S. mark is involved. Hence, *MO* should always favor a U.S. forum when it holds a U.S. mark. Additionally the *UV* difference between situation I in table B (having U.S. mark) and situation II in table B (having foreign mark) is very significant.³⁹³

The conclusion derived from tables A and B is that *Rs* should always favor bringing RDNH actions in U.S. courts,³⁹⁴ while *MOs* should also favor the U.S. forum, but only when defending U.S. marks. Another interesting aspect of the model can be demonstrated by combining the results of tables A(a) and B(b). It appears that plaintiffs in general are expected to favor a U.S. forum in six out of eight possible scenarios. Assuming that every scenario has the same probability to occur, the model suggests that plaintiffs are expected to favor litigation in the United States in

³⁸⁹ The total utility value (*TUV*) is 4.5 compared to only 3 in *Jurisdiction X*.

³⁹⁰ In all four possible alternatives *R*'s utility value (*UV*) is higher in the United States than in *Jurisdiction X*.

³⁹¹ The *TUV* is 5.5 in the United States, and 4 in *Jurisdiction X*, compared to 4.5 and 3, respectively.

³⁹² *MO* has *TUV* 3 in both venues.

³⁹³ In situation I in table B, the *UV* is 2.5. In situation II, the *UV* is only 0.5.

³⁹⁴ This assumes sterility of the scenario, namely that only the three arguments of personal jurisdiction, subject matter jurisdiction, and merits are controlling *R*'s litigation decision.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 109

approximately seventy-five percent of the cases.³⁹⁵ This finding indicates that the ACPA has the potential of becoming a “plaintiffs’ magnet” in cybersquatting disputes.³⁹⁶

b) The IACT World

Table C
R’s Alternatives in an IACT World

Situation	United States		<i>Jurisdiction X</i>	
	I	II	III	IV
<i>TM</i>	+	–	+	–
<i>PJR</i>	1	1	1	1
<i>SMJ</i>	1	1	1	1
<i>Merits</i>	0.5	0.5	0.5	0.5
<i>UV</i>	2.5	2.5	2.5	2.5
<i>TUV</i>	5		5	

Table D
MO’s Alternatives in an IACT World

Situation	United States		<i>Jurisdiction X</i>	
	I	II	III	IV
<i>TM</i>	+	–	+	–
<i>PJR</i>	1	1	1	1
<i>SMJ</i>	1	1	1	1
<i>Merits</i>	0.5	0.5	0.5	0.5
<i>UV</i>	2.5	2.5	2.5	2.5
<i>TUV</i>	5		5	

i. Explanation

Tables C and D present a reality possible in a world adhering to the IACT regime. In table C, *R* files a RDNH action in either the United States or *Jurisdiction X* and is likely to have in both

³⁹⁵ $6 \times 0.125 = 0.75$.

³⁹⁶ This conclusion correlates with a previous finding indicating that the vast majority of court-challenged UDRP decisions are litigated in the U.S. courts. *See supra* note 316 and accompanying text. This correlation, however, does not necessarily suggest that the situation described by the model is the *only* explanation for that finding.

jurisdictions *PJR* and *SMJ* afforded by the IACT.³⁹⁷ Moreover, no matter whether the mark in question is potentially protected in the United States, in *Jurisdiction X*, in both, or in neither, *R* only *may* succeed on the merits, therefore the value 0.5 assigned.³⁹⁸ Regarding the merits question, the adjudicating court's cybersquatting standard is generally applied,³⁹⁹ while the substantive trademark laws applied in deciding whether the mark is an IACT mark are U.S. law, *Jurisdiction X* law, or both.⁴⁰⁰ The situation is essentially identical from *MO*'s perspective. It should be able to assert personal and subject matter jurisdictions in cybersquatting claims in any member state, and without regard to whether the adjudicating member state substantively recognizes the mark. *MO*'s success on the merits depends on showing that (1) *MO* holds an IACT mark; (2) *R* does not hold an IACT mark; and (3) registration is unlawful under the applicable cybersquatting standard.

ii. Analysis

Tables C and D clearly present meaningful change of positions of potential plaintiffs. Regardless of the nature of the trademark rights involved and regardless of the venue adjudicating the dispute, plaintiffs, both *R* and *MO*, have the same *UV*s and *TUV*s. Namely, tables C and D show that plaintiffs, in any possible scenario of cybersquatting disputes, are venue indifferent.

This result is achievable because the subject matter jurisdiction and the personal jurisdiction problems are solved uniformly by the IACT structure in a vast majority of possible situations. The IACT system would have a substantial impact on several negative aspects of the present scheme. First, an identical *UV* in all jurisdictions, regardless of the nationality of the mark or the type of plaintiff, is

³⁹⁷ Subject matter jurisdiction is afforded by virtue of the anti-cybersquatting legislation provided according to principle 1. In addition, *R* should not experience difficulties in establishing personal jurisdiction, absent of bad faith situation, in accordance with principle 10.

³⁹⁸ Compare this with situation II in tables A and B, where the merits values are 1 and 0, respectively. See *supra* Part V.C.2 tbls. A, B.

³⁹⁹ The standard is generally applied in accordance with principle 3, but subject to the choice of law principles.

⁴⁰⁰ The applicable trademark law depends on the nature of the trademark rights asserted by *MO*.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 111

expected to discourage plaintiffs from attempting to direct the dispute to the national courts most suitable for their needs. Additionally, since the result in the various national courts depends on similar considerations, the motivation to employ litigation strategies by exploiting the ill-structured UDRP procedural rules should disappear. Furthermore, the IACT scheme, through its choice of law principles, decreases the potential benefits for plaintiffs to forum shop under protective standards applied in different member states.⁴⁰¹

Second, the laundry machine effect⁴⁰² in RDNH cases involving foreign marks litigated in U.S. courts under the ACPA disappears. Since under the IACT, U.S. courts must recognize and enforce foreign trademarks that constitute IACT marks *for the limited purpose of preventing cybersquatting*, owners of these marks would no longer stand in U.S. courts without redress. Clearly, in an IACT world no other member state would be allowed to legislate a scheme that results in the laundry machine effect of U.S. or foreign marks. In such a world, the concept of fairness is better served, and national courts are expected to experience less difficulty in consolidating international comity principles and national cybersquatting schemes.

Third, owners of foreign marks are no longer endangering their long-term interests by filing a UDRP (or any other similar policy) complaint. The partial reverse effect,⁴⁰³ contemplating the apprehension of owners of foreign marks from filing UDRP complaints in a post-*Barcelona.com* reality, is no longer a valid concern. Absent of disfavoring treatment in U.S. courts, the possible exercise of the ACPA's RDNH provision is not substantially different than a UDRP review in any other member state's national court.

Finally, the IACT system could help in preventing litigation races. Such a phenomenon is a valid concern bearing some consequences where different national legal schemes have possible

⁴⁰¹ See *supra* text accompanying 253–54 (discussing principles 6 and 7).

⁴⁰² See *supra* Part IV.D.4.

⁴⁰³ See *supra* Part IV.C.3 (describing a contemplated phenomenon of foreign owners avoiding the UDRP and by doing so trying to avoid the long arm of the RDNH provision).

application on a single dispute. In this context, when comity allows⁴⁰⁴ the first court where the case was brought to adjudicate the dispute, parties are discouraged from turning to litigation alternatives first.⁴⁰⁵ Moreover, the increase in certainty provided by the IACT system regarding litigation outcomes should result in a reduction of cybersquatting litigation volume in general, and encourage parties to turn first to alternative dispute resolution mechanisms.

It is important to note that an IACT scheme does not render the UDRP meaningless or unnecessary. The UDRP may remain an important mechanism providing a fast, cheap, and effective solution in simple and straightforward cases of cybersquatting. When disputes are no longer simple and straightforward, the IACT scheme also may be considered as providing a legitimate appeal or judicial review forum on UDRP decisions. Unlike the present judicial review option, however, which is highly forum-sensitive, applicable law-sensitive and subject to potential manipulations and strategies, an IACT forum adjudication is none of the above. Consequently, the UDRP may transform from a forum shopping and RDNH engine into a component in a system that is designed, *inter alia*, to thwart these problems.

Chicago-Kent Law Professor Graeme B. Dinwoodie concluded that “[t]he rules that will control the allocation and use of domain names . . . will inevitably (and perhaps appropriately) reflect laws that are national, international, and supranational in nature. They will be developed in quasi-legislative and quasi-judicial fora that are national, international, and supranational in nature.”⁴⁰⁶ Concurring with this observation, it might be said that the IACT scheme is making one step in this direction. The IACT represents a solution that is no more than an essential combination of national

⁴⁰⁴ In this context, comity means in accordance with certain courts’ in rem jurisdiction rules.

⁴⁰⁵ See *supra* Part IV.D.3 (discussing the “litigation race” as a consequence of the first-in-right rule as applied in *GlobalSantaFe*).

⁴⁰⁶ Graeme B. Dinwoodie, *(National) Trademark Laws and the (Non-National) Domain Name System*, 21 U. PA. J. INT’L ECON. L. 495, 521 (2000).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 113

laws, an international treaty, and preliminary supranational mechanisms in place.⁴⁰⁷

D. Why Should the IACT Be Attractive to Internet Nations?

1. Everyone Gets a Slice of the Pie

The analysis laid out in this Article suggests that an IACT scheme has the potential of solving many of the present scheme's shortcomings. Realistically, it is important to consider whether the IACT would provide an advantageous and attractive alternative to any national player involved. The argument is that an IACT structure should be, in many respects, attractive both to the United States and to other foreign states. More specifically, foreign countries' incentive to join an IACT of which the United States is a member state is clear; trademark rights protected under their laws would no longer have high potential to receive disfavoring treatment by a U.S. court deciding on cybersquatting disputes under the ACPA. Owners of foreign marks would no longer be "stripped" of their trademark rights in RDNH cases in U.S. courts.⁴⁰⁸ Additionally, many of the concerns regarding the ACPA in rem provision and its potential adverse effect on foreign interests should diminish under an IACT structure.⁴⁰⁹ Consequently, some highly problematic countermeasures such as the legislation of competing national anticybersquatting laws or the creation of a competing DNS infrastructure altogether, would not be necessary in this context.⁴¹⁰

⁴⁰⁷ Dinwoodie asserted that "[t]he UDRP holds the promise of supranational laws and supranational adjudication." *Id.* at 511 (footnote omitted). In this respect, the UDRP (or any other similar international dispute resolution mechanism concerning rights in domain names) is the supranational aspect of the general IACT scheme, providing limited solutions in limited types of fact patterns.

⁴⁰⁸ The city council argued in *Barcelona.com* that adjudicating the dispute only according to U.S. law would strip a trademark owner of its foreign rights whenever it is hauled into court by a U.S. domain name owner who has lost a UDRP administrative proceeding. *See Barcelona.com, Inc. v. Excelentísimo Ayuntamiento de Barcelona*, 330 F.3d 617, 622–23 (4th Cir. 2003).

⁴⁰⁹ *See* discussion *supra* Parts II.B.2, IV.D.

⁴¹⁰ *See* discussion *supra* Part IV.E (discussing some possible foreign reactions to U.S. policy in regulating and adjudicating domain name registrations).

On the other hand, the United States may also find the IACT to be a better alternative. It would reduce the antagonism and negative sentiments emerging in other countries toward its rulemaking policy and courts.⁴¹¹ Additionally, preventing various types of foreign reaction, motivated by those sentiments, would also serve U.S. interests.⁴¹² Finally, the United States in particular should benefit from the expected general reduction in the volume of cybersquatting litigation. Such general reduction is likely to ease the burden of caseload on U.S. federal courts, especially the ones in Virginia. Regarding disputes that nevertheless end up in court, a more internationally oriented scheme, affording plaintiffs with the opportunity to bring the dispute in any member state's court without risking their interests, would distribute adjudication more proportionally between the jurisdictions involved.

2. IACT Critique

The IACT is, by no means, a perfect solution to international domain name disputes. Some problematic aspects are yet to be solved. For example, the minimum standard concept mandated by principle 2 is expected to cause concerns among some potential member states. Generally speaking, reaching an international consensus regarding any kind of intellectual property standard of protection has proven hard to achieve.⁴¹³ Different countries have different views about the nature and purpose of intellectual property laws. In the case of trademarks, U.S. law is aimed at protecting consumers against confusion and aggressively protecting the proprietary interests of mark owners, driven by the desire to encourage entrepreneurship, investments, and individual efforts. On the other hand, in countries like Japan, intellectual property policy is generally driven by commitments toward collective benefits and progress of the nation as a whole.⁴¹⁴

⁴¹¹ See Rains, *supra* note 335.

⁴¹² See *supra* Part V.A (analyzing the U.S. unilateral approach as a lose-lose situation).

⁴¹³ See generally Marney L. Cheek, *The Limits of Informal Regulatory Cooperation in International Affairs: A Review of the Global Intellectual Property Regime*, 33 GEO. WASH. INT'L L. REV. 277 (2001) (investigating the global intellectual property rights regime with a specific focus on the process of international consensus building).

⁴¹⁴ Yonehara, *supra* note 331, at 213–14 (describing the policy rationales of Japanese intellectual property laws).

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 115

Different views about the role of trademark law created different legal definitions of marks and dictated a different scope and type of protection. Such differences may render an internationally accepted minimum standard an evasive concept.⁴¹⁵

Another thorny issue, relevant in any attempt to regulate domain name registration, is the issue of well-known marks.⁴¹⁶ The proposed IACT does not distinguish between marks on basis of their strength. Principle 9 sets the first-in-time rule, providing that when two IACT marks are competing on the same domain name, the first mark owner to register wins. That means that domain name registration of a lesser known mark recognized by one of the member states would prevail over a claim of a well-known mark regarding the registration as long as the lesser known mark registered the domain name first. There is no easy solution to this problem, especially since it goes down to the heart of the controversy regarding the appropriate scope of trademark protection, particularly in the context of the Internet, where domain names are global and unique.⁴¹⁷

⁴¹⁵ A prominent attempt to reach internationally accepted standards on this issue was made in WIPO's 1999 report on Internet domain names. See WIPO FINAL REPORT, *supra* note 355, ¶¶ 129–204. The enforcement of the WIPO recommendation (after some revisions and modification), however, was effectuated by ICANN not by virtue of international consensus, but because of ICANN's control over the domain name system. See *supra* Part II.A.1 (describing the adoption of the UDRP by ICANN and its imposition through registration agreements on all gTLD registrations).

⁴¹⁶ The Lanham Act terminology for a well-known mark is “famous mark.” See 15 U.S.C. § 1125(c)(1) (2000). Famous marks are protected against uses that “cause[] dilution of the distinctive quality of the mark.” *Id.* Under the Lanham Act, dilution can occur even when there is no likelihood of confusion, mistake, or deception. See *id.* § 1127 (defining “dilution”). The FTDA added to the Lanham Act a non-exhaustive list of circumstances, helping courts to determine whether a mark in question is famous or not. See *id.* § 1125(c)(1)(A)–(H). In international fora, article 16(2) of the TRIPS Agreement, referring to article 6*bis* of the Paris Convention, mandates that “[i]n determining whether a trademark is well-known, Members shall take account of the knowledge of the trademark in the relevant sector of the public, including knowledge in the Member concerned which has been obtained as a result of the promotion of the trademark.” TRIPS, *supra* note 351, art. 16(2). Article 16(3) extends protection of well-known marks also to use in “goods or services which are not similar to those in respect of which a trademark is registered.” *Id.* art. 16(3).

⁴¹⁷ The WIPO Final Report devoted a detailed and lengthy analysis to this problem. See WIPO FINAL REPORT, *supra* note 355, ¶¶ 245–303. It suggested creating a priority scheme that would favor well-known or famous marks in registration under some or all the gTLDs. *Id.* ¶¶ 276–303. This recommendation, however, was not adopted by ICANN

Despite these problems and perhaps some others that are not discussed here, this Article argues that crafting an IACT, tailored around the ten principles described above, is partially achievable. There are three major reasons supporting this argument. First, the IACT does not interfere with national substantive trademark protection. In other words, a member state should be free to keep its substantive trademark law framework unchanged—most importantly, its definition and scope of marks eligible for protection.⁴¹⁸ Next, a member state should not be required to automatically grant full protection to marks that are protected by other member states. Protection of non-recognized IACT marks extends only to adjudication of domain name disputes, no more and no less. A final reason supporting the IACT's achievability is that especially today, when the shortcomings of the present system are no longer merely theoretical or academic but real and acute, there is hope that Internet nations will show more flexibility and motivation in bridging the controversies and crafting together a new, better platform for international dispute resolution, at least in the context of domain names.

CONCLUSION

The *Barcelona.com* decision is a correct application of a problematic law. It contributes to the formulation of legal reality in which U.S. federal courts, in some situations, constitute a friendly forum to U.S. mark owners and potential cybersquatters of foreign marks. At the same time, U.S. federal courts are becoming hostile to owners of foreign marks trying to protect their marks against cybersquatting under the ACPA RDNH provision. Such reality is likely to bring about many worrisome developments in the near future. On the individual, small-scale level, which may evolve into a general trend, the possible result could be that parties

and thus, was not included in the UDRP. *See* Froomkin, *supra* note 69, at 632 (noting that ICANN did not adopt WIPO's proposal regarding a pre-emptive protection to famous or well-known marks). In some gTLDs, however, ICANN implemented a "sunrise" policy, which gave *all* trademark holders some sort of pre-emptive registration rights. *Id.* at 632 n.91.

⁴¹⁸ Clearly, *some* trademark protection would be a prerequisite for joining the IACT structure. *See supra* note 354 and accompanying text.

2003] *BETTER MODEL FOR INTERNATIONAL DOMAIN DISPUTES* 117

to international domain name disputes would direct litigation to the forum that entertains their claims according to domestic, favorable rules. Given the present physical structure of the Internet and the structure of Internet-related rules, however, a large-scale reaction of other Internet nations may bring about even more troubling and radical results. The outcome in the *Barcelona.com* case underlines the faults of a unilateral approach to domain name regulation and adjudication. That approach has proven itself to be inadequate, bearing myriad negative ramifications. At the same time, the *Barcelona.com* decision reemphasizes the need for an international collaboration in the battle against cybersquatting activities. The proposal for the International Anticybersquatting Treaty represents an alternative approach that should better serve the underlining objective of fairly and adequately adjudicating international cybersquatting disputes.