Regulating Cybersquatting on the Information Super Highway

By

Richard Symmes

Introduction

The internet has become a tool of both the common man and Fortune 500 corporations. Beginning in the early 1990s, when regulation was minimal and government intervention was scarce, many high profile corporations were unaware of the impact the internet, let alone the registration of domain names would have in the future. In 1994 journalist Joshua Quittner of Wired Magazine foreshadowed the legal battles that would take place in the next few years.[1] Quittner was able to obtain the domain name of McDonalds back in 1994 by doing very little, and even warning the company that he was going to register their trademark as a domain name. At the time McDonalds could have cared less, today however everything would be very different. Quittner discovered while researching that only one third of Fortune 500 companies had registered domain names, while other entrepreneurs owned 14 percent of American companies' domain names.[2] The remaining 50 percent of the Fortune 500 companies' domain names were available for the taking. Anybody who knew how to register a domain name was now in business. This trend would soon change as almost all multinational companies as well as any other company with business sense now possesses their own website and domain name. Companies today are also very protective of these trademarks and domain names and

[1] Joshua Quittner, Billions Registered: *Right Now, There Are No Rules to Keep You From Owning a Bitchin' Corporate Name As Your Own Internet Address*, Wired, Oct. 1994, http://www.wired.com/wired/archive/2.10/mcdonalds.html.
[2] *Id.* at 54.

litigate and use arbitration in order to solve domain name disputes. It took until 1999 for any type of regulation of the internet to occur. It was the United States who finally took notice of what a powerful tool the internet has become in terms of the amount of information provided and the broad audience that it is capable of reaching. The result was the enactment of the Anticybersquatting Consumer Protection Act ("ACPA"). The rest of the world has been sluggish to adopt specific cybersquatting regulations within their nations and countries have opted to rely on the World Intellectual Property Organization ("WIPO") and an arbitration process known as the Uniform Dispute Resolution Policy ("UDRP") in addition to attempting to apply their own general trademark laws with special amendments to cybersquatting. The result makes litigating a cybersquatting case very difficult in foreign nations because the laws are not specific to cybersquatting, which causes many jurisdictional issues.

Cybersquatting is defined as the act of "reserving a domain name on the internet, especially a name that would be associated with a company's trademark, and then seeking to profit by selling or licensing the name to the company that has an interest in being identified with it."[3] In the early 1990s, many entities began buying domain names of well-known corporations as well as misspelled corporate names and celebrity names so that they could make a quick buck through web surfers' mistakes or curiosity.[4] The cybersquatters even received money from the corporations to transfer the domain names to themselves in order to avoid confusion among their web visitors. Many of these

[3] Bryan A. Garner, *Blacks Law Dictionary Second Pocket edition 169* (West Publishing Co. 2001) (1996).
[4] Many celebrities and companies have sued to protect their rights in their domain names, which is discussed later in this paper. Some of these companies include Microsoft and Venetian Casino Resorts. In 2006 WIPO decided cases for Adidas, Blockbuster, Gateway, Honda, and Wal-Mart on the company side and Tom Cruise, Jimmy Kimmel, Martha Stewart and Xzibit on the celebrity side. WIPO UDRP Domain name cases, available at http://www.wipo.int/amc/en/domains/cases/all.html, (last visited on October 1, 2006).

cybersquatter websites often contained adult imagery that was not suitable for children or advertisements that redirected a user to another website so that the cybersquatter could make a profit from advertisements.[5] With no rules in place, the corporations or celebrities were left with no choice but to buy out the cybersquatters in order to obtain the domain names and save their respective reputations so that they would not be confused with the cybersquatters' websites.

This paper will compare and contrast how the ACPA has affected individuals and corporations both domestically and abroad, as well as how celebrities and corporations have utilized the UDRP. (The UDRP allows for jurisdiction to be obtained easier as compared to United States laws, while also providing a shorter and cheaper process for settling domain name disputes in the form of alternative dispute resolution). This paper will then explore how cybersquatting cases are handled in the Pacific Rim, and the success of these efforts. In the long run, the rest of the world needs to catch up to the United States when it comes to enacting rules pertaining to cybersquatting. There needs to be a general rule that all countries can follow together to prevent chaos and jurisdictional issues from interfering in domain name disputes. Currently, however, the United States has laid the groundwork for other countries to follow so that each country can enact appropriate cybersquatting laws. The world as a whole is moving in the right direction in terms of preventing cybersquatters before they even think about registering a trademarked name. Now the rules have to be refined to make the best laws to protect against cybersquatting.

[5] Marcy Zitz, Fighting Back Against Cybersquatters (2000), no longer available at http://familyinternet.about.com/library/weekly/aa082100a.htm (this article described the art of cybersquatting, the rules that apply and who has been involved in such disputes recently and in the past).

The Development of Internet Regulation

In 1994, the only way a domain name could be registered was through the Internet Network Information Center ("InterNic"). At the time, only two full time employees and one part-time employee registered names.[6] The only reason a domain name request was denied was if InterNic determined the name was already in use or it was very obvious that a person was not entitled to the name.[7] It was up to the registrant to determine if there was any trademark infringement.

Today there are many companies that register domain names for a fee and all work with "The Internet Corporation for Assigned Names and Numbers ("ICANN"), who is responsible for managing and coordinating the Domain Name System ("DNS") to ensure that every address is unique and that all users of the internet can find all valid addresses."[8] ICANN does this by overseeing the distribution of unique IP addresses and domain names and ensuring that each domain name maps to the correct IP address.[9] This allows for one organization to oversee the main registration of internet domain names rather than having several regulators. ICANN is also responsible for accrediting the domain name registrars. To "[a]ccredit means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those

[6] Joshua Quittner, *Billions Registered: Right Now, There Are No Rules to Keep You From Owning a Bitchin' Corporate Name As Your Own Internet Address*, Wired, Oct. 1994 at 54.
[7] Joshua Quittner, *Billions Registered: Right Now, There Are No Rules to Keep You From Owning a Bitchin' Corporate Name As Your Own Internet Address*, Wired, Oct. 1994 at 54.
[8] Internet Corporation for Assigned Names and Numbers FAQs, http://www.icann.org/faq/#howregister (last visited Sept. 17, 2006).
[9] *Id*.

standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of registrar services."[10]

In 1999, the U.S. government decided that it was time to prevent individuals from being able to profit off another's trademarked name by regulating cybersquatting. The result was the Anticybersquatting Consumer Protection Act of 1999 (ACPA).[11] Under the ACPA, a person shall be liable in civil action by the owner of a mark if an infringer has a bad faith intent to profit from that mark, the mark first in use is distinctive or famous, and the mark is identical or confusingly similar to the mark already in use.[12]

---

[10] *Id.* (this makes sure the proper people are registering the right domain names).

[11] 15 U.S.C. § 1125(d) (1999)

[12] 15 U.S.C. § 1125(d)(1)(A) (2006). This statute lays out the factors of the ACPA that will be used to determine if somebody is guilty of cybersquatting. A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person (i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and (ii) registers, traffics in, or uses a domain name that (I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark; (II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or (III) is a trademark, word, or name protected by reason of section 706 of Title 18 or section 220506 of Title 36.

[13] 15 U.S.C. § 1125(d)(1)(B)(i) (1999)

> In determining whether a person has a bad faith intent described under subparagraph (a), a court may consider factors such as, but not limited to:
>
> (I) the trademark or other intellectual property rights of the person, if any, in the domain name;
>
> (II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
>
> (III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
>
> (IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
>
> (V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
>
> (VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
>
> (VII) the person's provision of material and misleading false contract information when applying for the registration of the domain name, the person's initial failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

The ACPA has determined nine factors to be used to determine if a mark has been used in bad faith to profit. These factors are focused on preventing an individual or organization from using the trademark rights of another in order to make a profit.[13] To meet the second factor under the ACPA's test, a mark is considered distinctive or famous if it is used in commerce and has a secondary meaning or is inherently distinctive because the mark is arbitrary, fanciful or suggestive. Also certain types of trade dress such as product packaging are inherently distinctive.[14] Finally to meet the third factor of the ACPA test a confusability analysis must be used. In order to determine if a trademark is confusingly similar each circuit has determined factors for judges to weigh whether a trademark is confusingly similar to another. These factors may range between eight and thirteen factors.[15] In the ninth circuit eight factors are used to determine if a mark is identical or confusingly similar to a mark already in use.[16]

Another aspect of the ACPA that makes it unique is that it allows for *in rem* jurisdiction over foreign infringers. In an *in rem* action, the court asserts personal jurisdiction over a defendant's property that he owns rather than a defendant's person.

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous.

[14] Two Pesos v. Taco Cabana, 505 US 763 (1992) (the Supreme Court ruled that a non functioning trade dress could be inherently distinctive and not require secondary meaning).

[15] United States Trademark Law, http://en.wikipedia.org/wiki/United_States_trademark_law (last visited Dec. 15, 2007).

[16] AMF Inc. v. Sleekcraft Boats, 599 F.2d 341, 348-349 (9th Cir. 1979) (factors used to determine if a mark is confusingly similar to another mark already in use include strength of the mark; proximity of the goods to one another; similarity of the marks; evidence of actual confusion; marketing channels used; type of goods and the degree of care likely to be exercised by the purchaser; defendant's intent in selecting the mark; and, likelihood of expansion of the product lines).

This makes it easier for a court to gain jurisdiction over a person if they live outside the country.[17] In ACPA cases, this property consists of the domain names in question if they were registered in the United States.[18] If the domain name was registered in the United States, then a suit may be brought in the district where the domain name registrar or domain name registry is located.[19] In order to make use of the *in rem* provision, the ACPA requires a plaintiff prove that he or she used due diligence in trying to find the defendant to obtain *in personam* personal jurisdiction but was unsuccessful.[20] Due diligence may consist of any legitimate effort to track somebody down so that service of process can occur.

ACPA Applied Domestically

Since the ACPA was incorporated into United States trademark law in 1999 many large high profile domestic companies have sued to have their rights protected. Recently some of these companies have included Venetian Casino Resort and Microsoft. In *Venetian Casino Resort, LLC v. VenetianGold.com,* Venetian Casino Resort (VCR), a hotel and casino resort that operates in Las Vegas, Nevada, sued Vincent Coyle and VenetianGold.com under the ACPA,[21] "alleging that defendant domain names [were] confusingly similar to plaintiff's trademarks [and] … that the registrant of the defendant domain names had a bad faith intent to profit from the marks."[22] One cannot register a domain name that is confusingly similar to a registered trademark with a bad faith intent

[17] Shaffer v. Heitner, 433 U.S. 186 (1977) (landmark case that states the rule for *in rem* jurisdiction to take place).
[18] 15 U.S.C. § 1125(d)(2)(A).
[19] *Id.*
[20] 15 U.S.C. § 1125(d)(2)(A)(ii)(II).
[21] 15 U.S.C. §1125(d)(1)(A).
[22] Venetian Casino Resort, LLC, 380 F. Supp. 2d 737 (D. Va. 2005*)*, at 743.

to profit from it. VCR had at least 15 United States trademarks registrations for its service marks,[23] 10 of which were issued before Vincent Coyle and Global DIP registered their seven domain names,[24] which "link to a website offering worldwide casino-type gaming services on the internet."[25] Furthermore, Vincent Coyle was aware of VCR in Las Vegas before he registered any of the defendant domain names. The VenetianGold.com website was launched in 2001 and maintained its servers in Costa Rica while Coyle operated the business from the United Kingdom.

The court looked to many elements of the ACPA, which included the factors outlined in 15 U.S.C. § 1125(d)(1)(A) (1999), listed in the footnotes above, as well as nine additional factors from the ACPA found in 15 U.S.C. §1125(d)(1)(B) (1999), to determine whether a person has a bad faith intent. The major factors to consider, among others, included whether a person has the trademark or other intellectual property rights in a domain name, the extent to which the domain name consists of the legal name of the person, whether a person offers to transfer, sell, or otherwise assign the domain name to the mark owner or any third party financial gain, and the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names.[26]

The court ruled for the plaintiff, VCR, after deciding that the Venetian marks were distinctive and that Venitiangold.com and the other defendant domain names were

---

[23] *Id.* (trademarks include: Venetian, The Venetian, The Venetian Hotel Resort Hotel Casino.
[24] VenetianGold.com, VenetianGold.net, VenetianGoldCasino.com, VenetianGoldCasino.net, VenecianGold.com, VeniceGoldCasino.com, and VenicianGold.com).
[25] Venetian Casino Resort, LLC, 380 F. Supp. 2d at 739.
[26] *See supra* note 13 (describing the full nine factors used from 15 U.S.C. §1125(d)(1)(b) (1999), to determine bad faith).

confusingly similar in sight, sound, and meaning to the plaintiff's marks. The court also ruled that the registrant of the defendant domain names had a bad faith intent to profit from plaintiff's marks.[27] The court also relied on *Harrods Ltd v. Sixty Internet Domain Names,* which stated the "most important grounds for finding bad faith are the unique circumstances of the case, which do not fit neatly into the specific factors enumerated by Congress but may nevertheless be considered under the statute."[28] Every case may be determined differently depending on the specific situation and facts, even if the same factors are being applied.

In the VCR case, the plaintiffs were able to satisfy enough of the ACPA factors the court used for consideration as well as obtain the domain names that were harmful to their business. This case is able to demonstrate how the ACPA works, and that in most cases big corporations with trademarked names will be protected from cybersquatters in a court of law.

Another large domestic corporation that fought a legal battle over cybersquatting was Microsoft. The Redmond, Washington company filed three lawsuits against cybersquatters on August 22, 2006. According to Microsoft, 2,000 domain names that targeted the company were being registered each day.[29] In response, Microsoft filed three civil lawsuits against four defendants it said were profiting from domain names that infringed on Microsoft trademarks. One lawsuit filed in U.S. District Court in Utah

---

[27] Venetian Casino Resort, LLC, 380 F. Supp. 2d at 740.
[28] Harrods Ltd v. Sixty Internet Domain Names, 157 F. Supp.2d 658, (E.D. Va.2001), at 666 *(*quoting Sporty's Farm, LLC v. Sportsman's Market, Inc., 202 F.3d 489, 499 (2d Cir.2000)).
[29] Associated Press, Microsoft Sues Cybersquatters, http://www.msnbc.msn.com/id/14470091/ (last visited Sept. 22, 2006) (noting that this article describes the legal battles that Microsoft is going through in order to protect their trademarks and domain names).

alleged that three defendants together registered 324 domain names directed at Microsoft and their trademarks.[30] The 324 domain names related to Microsoft are a numerous number of names for people to register in the hopes of capitalizing off of the name of another. These names will most likely be transferred over to Microsoft in the near future or have already been transferred. In the second lawsuit, Microsoft alleged that Partner IV Holdings, registered 85 domain names involving Microsoft and its trademarks.[31] These suits were filed in the U.S. District Court in California. Finally Microsoft filed a "John Doe" lawsuit in the United States District Court in Washington. The final lawsuit targeted cybersquatters who conceal their identities in order to avoid legal action.[32] Look for Microsoft to issue subpoenas to domain name registrars in the near future. Microsoft also plans to sue under ACPA and attempt to impose fines up to $100,000 as well as attorney fees, the maximum penalty allowed by the law,[33] on anybody who hoped to profit off the domain names in bad faith. In the future, it will be interesting to see how these cases turn out, but I think it is safe to say that Microsoft and other companies trying to protect their trademarks have a good cause of action since these cybersquatters are trying to make a profit in bad faith off of their trademarked names.

The courts do not always find bad faith and force domain name holders to transfer their domain names to somebody else under the ACPA. In *Lamparello v. Falwell*, Christopher Lamparello registered the domain name “www.fallwell.com” in order to voice his opinions regarding Reverend Jerry Falwell’s points of view, more specifically his perspective about homosexuals. “The site contained in-depth criticism of Reverend

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] 15 U.S.C. § 1125(d).

Falwell's views."[34] Also the homepage prominently stated that, "[t]his website is NOT affiliated with Jerry Falwell or his ministry; advised if you would like to visit Rev. Falwell's website, you may click here."[35] Criticizing an individuals view over the internet is a form of free speech, and also does not involve one trying to make a profit in most cases. Therefore bad faith would be hard to prove. Also the warning on the webpage seems to be adequate to would be viewers of the webpage that Falwell is not affiliated with the page. Lamparello sought a declaratory judgment of non-infringement but Falwell counter claimed alleging infringement. This case is clearly different from the Venetian Casino Resort case or the Microsoft case since Lamparello was not looking to make a profit in bad faith or selling goods or services on his website. The court ruled for Lamparello after applying the ACPA's bad faith factors. The court held that "the use of a mark in a domain name for a gripe site criticizing the mark holder does not constitute cybersquatting."[36] This was a good ruling because there was no bad faith in terms of trying to make a profit and a person has the right to free speech on a web page. If somebody does not want to read the material on the webpage they don't have too.

These cases establish that suing under the ACPA does not always result in a ruling in favor of a trademark holder, only if it is found that a person has infringed in bad faith in order to make a profit.

How Foreign Companies are utilizing the American Cybersquatting Laws

[34] Lamparello v. Falwell, *420 F.3d 309 (4th Cir. 2005)* at 311.
[35] *Id*.
[36] *Id*. at 322.

Not only are domestic companies suing under the ACPA, but so are foreign corporations who feel that their trademarks are being infringed in the United States. In *Maruti v. Maruti Udyog Limited*, the plaintiff, Rao Tella (Tella) developed the website "maruti.com" and used the site as a search engine that allowed him to earn revenue through an affiliated website that paid him every time someone clicked an advertisement to reach another website. The defendant, Maruti Udyog Limited (Maruti), was incorporated under the laws of India where it has its principle place of business. The company had a registered trademark for Maruti in India and 19 other countries around the world and sold and exported its line of passenger cars to 70 countries around the world, not including the United States. Tella sought a declaratory judgment under the ACPA that his use of "maruti.com" was lawful. Maruti filed a counter claim alleging that Tella was a cybersquatter and violated the ACPA, alleging that Tella registered the domain name with a bad faith intent to profit from the use of the mark. Tella responded by claiming that the mark was not "used in commerce" in the United States, and was not entitled to the Act's protection.[37]

The court relied on a variety of cases in order to determine that foreign use of a foreign trademark creates no rights under United States law and that while, a trademark need not be federally registered in order to qualify for protection under the ACPA, the mark must be used in commerce. The court reasoned that "use in commerce can include foreign trade[, however,] … it must involve transactions between United States citizens and the subject of a foreign nation."[38] Since Maruti did not have a trademark that was used in commerce in the United States or in foreign trade with the United States, the

[37] Maruti v. Maruti Udyog Limited, No. L031478, 2006 WL 2422659 at 1 (D. Md. August 15, 2006).
[38] *Id*. at 3.

court ruled that Maruti did not have standing to bring its claim under the ACPA. This case represents the fact that a foreign corporation must have some kind of contacts with the United States in order to be able to be covered by the ACPA; however, it is questionable whether registering a domain name in the United States is enough contact to bring a suit against a foreign cybersquatter as the next two cases demonstrate.

Registering a domain in the U.S. may not always provide a company with jurisdiction to be protected by the U.S. laws, however, "[g]etting a court to assert personal jurisdiction over a defendant may not be difficult. A sophisticated registrant merely needs to register the domain name with a registrar having a principal office in the United States, supply that registrar with a United States address, and ensure that this address will show up in the registrar's Whois database."[39] The Whois database is used to identify registrants of domain names and can be accessed online through ICANN. *Barcelona.com Inc. v. Excelentisimo Ayuntamiento De Barcelona,* demonstrated how easy it is to gain standing in a United States court, even if both parties are foreign. In this case Joan Nogueras Cobo, a Spanish citizen, registered the domain name "barcelona.com," with the registrar Network Solutions in Virginia. Nogueras intended to turn barcelona.com into a tourist website and formed the company Bcom Inc. under Delaware law to own and run the website. "Although Bcom Inc. maintained a New York mailing address, it had no employees, office space, or telephone listing in the United States, and its server was in Spain."[40] Soon after Bcom Inc. was established, the

[39] Zohar Efroni, *The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: New Opportunities for International Forum Shopping?,* 26 Colum. J.L. & Arts 335, 362 (2003).
[40] Barcelona.com Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 620 (2003) (noting this case demonstrates why a company might want to obtain an American address, even if they don't use it for anything in order to be covered by the ACPA if a legal dispute shall arise).

Barcelona City Council in Spain, who owned 150 trademarks issued in Spain relating to the city of Barcelona, demanded the transfer of the domain name and invoked the Uniform Domain Resolution Policy (UDRP) to gain control of the domain name.[41] This policy is discussed in detail below and can be used to decide domain name disputes.

Through the UDRP and using Spanish law, the panel decided the domain name should belong to the Barcelona City Council. In response, Bcom Inc. filed a claim under the ACPA in United States federal court seeking a declaratory judgment that barcelona.com "does not infringe upon any trademark of defendant or cause confusion as to the origin, sponsorship, or approval of the website … and that the City Council is barred from instituting any action against Bcom Inc. for trademark infringement."[42] The district court, applying Spanish law, denied Bcom Inc.'s request for declaratory judgment. However Bcom Inc. subsequently "appealed under 15 U.S.C. § 1114(2)(D)(v), that it was entitled to have its conduct judged by United States law."[43] The United States court of appeals for the fourth circuit agreed, vacating, reversing and remanding the district court opinion, holding that Bcom Inc.'s registration and use of the name "Barcelona" was not unlawful because the city council never filed a counter claim disputing the issues in question.[44] This case represents just how easy it is for companies from around the world to be able to file claims in United States courts. The trend of foreign companies coming to the United States to file a claim is a trend that might

[41] *Id.* at 620-621 (noting that this case identifies the actions taken by the city of Barcelona in order to protect their own trademarks. The city went with the UDRP process because Spanish law did not provide enough protection from cybersquatters. They felt the UDRP was their best chance at protecting their trademarks).
[42] *Id.* at 621.
[43] *Id.* at 621-622. (noting that Bcom is entitled to United States law because of the business address and phone number they have in the United States).
[44] *Id.* at 628-630.

increase due to the number of countries lacking any specific cybersquatting laws similar to the ACPA. The ACPA can provide them with a better chance of protecting their interests and with a law equipped to deal with issues in cybersquatting.

In contrast, in *America Online Inc. v. Huang,* the court ruled that mere registration of a domain name is insufficient to constitute minimum contact.[45] In this case America Online (AOL) sued eAsia and its subsidiary Inforia Inc., which are California and Taiwan corporations, respectively, and "direct[ed] [their] products and services primarily, if not exclusively, at Chinese-speaking regions of Asia."[46] EAsia provided services similar to AOL in Asia and even provided an instant messaging service called "ICQ," which is exactly what AOL called its instant messaging service. What is in dispute is eAsia's registration and use of supposedly infringing domain names such as "picq.com", "picq.net", and Inforia Inc. registration of "cicq.net."[47] The domain names were registered with Network Solutions Incorporated ("NSI") in the state of Virginia of the United States. AOL contended that they had trademarked the term ICQ and that the defendants were infringing on that trademark through the registration of their domain names and sued in Virginia relying on the ACPA. EAsia moved for dismissal, arguing lack of personal jurisdiction, but AOL claimed that eAsia would have personal jurisdiction due to the fact that they registered domain names in Virginia. The court relied on *Burger King Corp. v. Rudzewicz*, which stated that "a defendant must have purposely availed itself of the privilege of conducting activities within the forum state to

[45] America Online Inc. v. Huang, 106 F. Supp. 2d 848 (E.D. Va. 2000).
[46] *Id*. at 850 (noting that defendants may not have directed its products at the United States in order to establish sufficient minimum contacts).
[47] *Id*. (noting that the registered names are very similar which is why America Online, Inc. is upset and feels that their trademarks have been infringed).

ensure that a defendant will not be brought into a jurisdiction solely as a result of random, fortuitous, or attenuated contacts."[48] The court ruled that eAsia did not purposefully avail itself of the benefit of the forum state and that they did not have a substantial connection with the forum state to provide sufficient minimum contacts.[49] The court came to this conclusion by looking at the domain name registration process. This process included: (1) entering into a standard registration agreement with NSI in Virginia, (2) contacting NSI in the course of registering the allegedly infringing domain names, but doing so via NSI's web page, using a computer located in either California or Taipei, Taiwan which can be seen as having minimal contact, (3) having brief transactions with NSI which involved minimal communication and no negotiation of provisions, (4) being involved in an agreement with NSI that created no reason for future communication between eAsia and NSI, in Virginia, other than the annual fee payment, and (5) "NSI did not hold itself out as a Virginia company and eAsia did not choose to register its domain names with NSI on the basis of its residency in Virginia. [Also,] it is possible that eAsia may not have even known the component of NSI with which it dealt was located in Virginia."[50] This case is different from the Barcelona case in the fact that Bcom Inc. meant to have their website seen in the United States so that tourists and others who wanted to research Barcelona in the United States would have easy access. They purposely availed themselves to the United States through the website by having a United States address, and registering the domain name in the United States, which is why the court ruled that there was jurisdiction. Every court is different and with new cybersquatting cases that

[48] *Id*. at 855-56 (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985)).
[49] *America Online Inc.,* 106 F. Supp. 2d at 857
[50] *Id*. at 856-57 (noting how the court determined that there was not enough contact with the United States to show that the registration of a domain name constitutes minimum contact with a forum state).

come out in the future, we might have a different result, depending on whether a court finds jurisdiction and minimum contacts with a state. Therefore, it is not always guaranteed that a company using the ACPA will be able to obtain jurisdiction to bring a defendant to court in the United States, even if a domain name is registered in this country.

However, foreign companies might hesitate when it comes to protecting their domain name interests in the United States under the ACPA. First, litigation in the federal courts is expensive and the case could be decided at a fraction of the cost using alternative means. Second, they will have to use the services of American counsel to file the federal complaint. Third, they must act quickly to prevent transfer of their domain name (especially if they have already lost a UDRP proceeding). Fourth, and perhaps most importantly, they will have to meet the ACPA standards for legitimate use of someone else's mark incorporated in their domain name, which are narrower than the UDRP's standards.[51] If a corporation cannot be covered by the ACPA or a corporation does not wish to use the ACPA, they have the option to seek arbitration through UDRP and organizations such as WIPO, which provides for some advantages in cost and timeliness.

An Alternative to the ACPA

In addition to going to court and applying the rules of the ACPA, there is an alternative tool which can be utilized in order to resolve cybersquatting issues. This alternative is called the Uniform Dispute Resolution Process ("UDRP"), which is

[51] Zohar Efroni, *The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: New Opportunities for International Forum Shopping?* 26 Colum. J.L. & Arts 335, 365 (2003).

overseen by the Internet Corporation for Assigned Names and Numbers ("ICANN"). When a person or company registers a domain name they must accept the terms of ICANN, which includes a provision about domain name disputes and using UDRP as a possible solution to a conflict.[52] ICANN is the result of the United States' 1998 "White Paper" study which "call[ed] for creation of non-for-profit corporation to handle consensus based technical management of the internet's infrastructure."[53]

The disputes are handled by approved dispute resolution service providers who follow the rules of the UDRP in addition to their own supplemental rules. The first and most popular provider to be approved by ICANN was the World Intellectual Property Organization ("WIPO"), which was approved in December 1999. The other providers in the order in which they were approved are: the National Arbitration Forum ("NAF"), Eresolution ("Eres"), CPR Institute for Dispute Resolution ("CPR"), and the Asian Domain Name Dispute Resolution Centre ("ADNDRC"), which has offices in Beijing and Hong Kong.[54] "Additional providers may be approved from time to time, however the above approvals are in effect until further notice."[55] It is always possible to find more providers, but for right now there seems to be enough to handle the work load.

The UDRP was first applied in December 1999 by WIPO in a case involving the World Wrestling Federation ("WWF") and the use of a domain name similar to their

---

[52] Internet Corporation for Assigned Names and Numbers, *Uniform Domain-Name Dispute-Resolution Policy* (1999), *available at* http://www.icann.org/udrp/udrp-policy-24oct99.htm.
[53] Internet Corporation for Assigned Names and Numbers, *Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy*, http://www.icann.org/udrp/udrp-schedule.htm (last visited September 26, 2006).
[54] Internet Corporation for Assigned Names and Numbers, *Approved Providers for Uniform Domain-Name Dispute-Resolution Policy*, http://www.icann.org/udrp/approved-providers.htm (last visited September 26, 2006).
[55] *Id*.

trademark by a private party. (The WWF won as the panel found that the infringer was using the domain name in bad faith in order to make a profit of the registration.)[56] "The UDRP has been adopted by all accredited domain-name registrars for domain names ending in .com, .net, and .org. It has also been adopted by certain managers of country code top level domains (e.g., .nu, .tv, .ws)."[57] Under the UDRP, an administrative panel has the power to cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of a registration agreement. Monetary compensation for infringement cannot be granted under the UDRP.

The UDRP process works much like filing a cause of action in a regular court. There is a complainant, who believes their trademark is being infringed upon, and a respondent who must respond to the allegations. In order for a case to proceed using the UDRP a complainant must prove that a respondent's (1) "domain name is identical or confusingly similar to a trademark or service mark in which the complainant has a right"[58], (2) that the respondent "has no rights or legitimate interests in the domain name"[59], and (3) the respondent's "domain name has been registered and is being used in bad faith."[60] In order to determine if a domain name is being used in bad faith, four factors are considered, which include circumstances indicating that the domain name has been registered or acquired

> primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark, [the

[56] World Wrestling Federation Entertainment, Inc. v. Michael Bosman, http://www.wipo.int/amc/en/domains/decisions/html/1999/d1999-0001.html.
[57] Internet Corporation for Assigned Names and Numbers: *Uniform Domain-Name Dispute-Resolution Policy* (1999), *available at* http://www.icann.org/udrp/udrp.htm (last visited September 26, 2006).
[58] *Id.* at http://www.icann.org/udrp/udrp-policy-24oct99.htm.
[59] *Id.*
[60] *Id.*

> potential infringer has] registered the domain name in order to prevent the owner of the trademark or service mark from using the mark in a corresponding domain name, the potential infringer has registered the domain name primarily for the purpose of disrupting the business of a competitor, and whether the potential infringer intentionally attempted to attract, for commercial gain, internet users to a web site by creating confusion with the complainant's trademark.[61]

UDRP administrative panels consist of either one or three panelists depending on how large a case is and whether or not a party requests that there be three panelists present or not. The number of panelists helps to determine the fees to be paid. "All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to th[e] policy shall be paid by the complainant, except in cases where [the respondent] elect[s] to expand the Administrative Panel from one to three panelists, … in which case all fees will be split evenly by [the respondent] and the complainant."[62] This billing process seems fair in the way it is structured. If one party wants additional panelists, they should have to pay for that convenience.

The fee schedules are competitive between providers, but WIPO, for instance, charges depending on how many domain names are involved and whether one or three panelists are used. With one panelist and between one and five domain names in dispute the cost is $1,500, with 6-10 domain names it is $2,000, and with more than 10 domain names in dispute, the cost is to be determined at a later date. With three panelists the

[61] *Id.* The full four factors that are used to determine bad faith in the UDRP are: (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 a 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 (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.

[62] *Id.*

costs go up significantly, with WIPO charging $4,000 for one to five domain names and $5,000 for six to 10 domain names in dispute.[63]

Another significant advantage of using UDRP rather than going to court under the ACPA, besides paying significantly less in fees, is that a case can be decided much faster since a panel can be assigned at anytime to decide the case. Hardly any waiting is required. "If neither the Complainant nor the Respondent has elected a three member panel, … the provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or at the lapse of the time period for the submission thereof, a single Panelist from its list of panelists."[64] If three panelists are requested then similar procedures are followed. "Once the entire panel is appointed, the provider shall notify the parties of the panelists appointed and the date by which, absent exceptional circumstances, the panel shall forward its decision on the complaint to the provider."[65] By keeping communication open with the parties, it helps keep both parties informed about what is occurring in their case. This is needed because under most circumstances there are no in person hearings under the UDRP, which include hearings by teleconference and videoconference. Only if the panel determines that such a hearing is necessary to decide the complaint will an in person hearing take place.[66] In person hearings are very rare and would require an exceptional circumstance such as if the case could not be decided otherwise. "All decisions by the panel, in the absence of exceptional circumstances are forwarded to the provider within fourteen days of its

[63] Schedule of Fees under the UDRP (valid as of December 1, 2002), http://www.wipo.int/amc/en/domains/fees/index.html (last visited October 1, 2006).
[64] Rules for Uniform Domain-Name Dispute-Resolution Policy, http://www.icann.org/udrp.udrp-rules-24oct99.htm, (last visited October 1, 2006).
[65] *Id*.
[66] *Id.* at rule 13.

appointment and in the case of a three member panel, the decision will be made by a majority."[67] The required majority decision in a panel of three helps to keep decisions fair so that there cannot be a tie. Also if a party believes that a panelist won't be on their side, they should request a three person panel to be sure that there is no bias and an impartial decision can be rendered. Also, "within three calendar days after receiving the decision from the panel, the provider shall communicate the full text of the decision to each party, the concerned registrars and ICANN."[68] This communication is done to help keep records of decisions and to see the reasoning behind every decision that a panel makes. After the decision is received, the registrar communicates to the parties, the provider and ICANN when the decision must be implemented – meaning when and if the domain names have to be transferred or cancelled. The amount of time that it takes to decide a case through UDRP is practically nothing considering that court cases can take years to decide, especially if there are appeals and discovery must be done. As a result, many companies and celebrities have decided to take advantage of the UDRP process as thousands of cases have already been decided to date. Another advantage of the UDRP process is that it may be applied to international corporations as well as domestic, which is something the ACPA has trouble with in terms of jurisdictional issues and not being able to get personal jurisdiction over international defendants.

How the UDRP is Affecting Large Companies and Celebrities

Many well known companies and celebrities had decided to use the UDRP system in order to protect their trademarks and names. In the past year, WIPO has decided cases

[67] *Id.* at rule 15(b).
[68] *Id.* at rule 16(a).

for Adidas, Blockbuster, Gateway, Honda, and Wal-Mart on the company side and Tom Cruise, Jimmy Kimmel, Martha Stewart and Xzibit on the celebrity side.[69] Other celebrities that have utilized the UDRP in the past have included "Madonna, Julia Roberts, Sting, Jethro Tull, Rita Rudner, Jimi Hendrix, Tina Turner and Don Henley."[70] In all of these cases, and in most situations, the domain names are transferred over to the complainant because the person who owned the domain names was acting in bad faith to make a profit off a trademark or name that did not belong to them. Every once in a while, however, a company or celebrity might not be able to transfer over a domain name. This was the case in 2000 when British rock star Sting was the complainant in a WIPO UDRP proceeding against Michael Urvan who had registered the domain name www.sting.com in 1995. The respondent asserted that "sting" is a general word in English and that registration of the domain would not violate any policies, that he had no intention to confuse the word "sting" with the singer Sting and that he is not a competitor with the singer Sting.[71] Also the respondent claimed he had been using the nickname

---

[69] WIPO UDRP Domain name cases, available at
(Adidas) http://www.wipo.int/amc/en/domains/decisions/html/2007/d2007-0032.html,
(Blockbuster) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0302.html
(Gateway) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0604.html
(Honda) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0190.html
(Wal-Mart) http://www.wipo.int/amc/en/domains/decisions/html/2007/d2007-0419.html
(Tom Cruise) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0560.html
(Jimmy Kimmel) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0402.html
(Martha Stewart) http://www.wipo.int/amc/en/domains/decisions/html/2007/d2007-0289.html
(Xzibit) http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0539.html (last visited on October 1, 2006).

[70] Marcy Zitz, *Fighting Back Against Cybersquatters*, no longer available at http://familyinternet.about.com/library/weekly/aa082100a.htm (last visited October 1, 2006).

[69] WIPO Arbitration and Mediation Center, Administrative panel decisions, Gordon Sumner, p/k/a Sting v Michael Urvan, Case No. D2000-0596, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0596.html (last visited on October 1, 2006).

sting for over eight years on the internet. The sole panelist agreed with the respondent and allowed Urvan to keep the domain name because it was not used in bad faith and that the word "sting" is a common word. The domain name, however, is currently used by the singer Sting as a fan site dedicated to the rock star and provides for a membership section, current events about Sting, ticket sales, a store dedicated to the singer, and allows users to access Sting's music.[72] This would mean that Urvan most likely sold his rights to the domain name to the rock star Sting or Ultrastar Entertainment, the company that owns and operates the website, after the WIPO decision was made.

How Pacific Rim Countries are Handling Cybersquatters

Although the internet was created in the United States, it is being used around the world by the majority of countries regardless of their size or if they are developed or developing countries. The Asian community in the Pacific Rim has recently given attention to the internet and cybersquatting as issues have began to arise overseas pertaining to the rights to domain names.

China has the largest population in the world with over 1.3 billion people and 123 million are considered internet users, which is second-most users behind the United States.[73] China also has its own country code for domain names, allowing users to register domain names ending in ".cn." This country code has been growing in popularity in recent years, with almost 1.2 million domain names registered ending in ".cn."[74] This number will continue to grow as the internet spreads throughout a country with one of the

[72] Sting, www.sting.com.
[73] China Internet Network Information Center, 18th Statistical Survey Report on the Internet Development in China (2006), http://www.cnnic.net.cn/download/2006/18threport-en.pdf.
[74] *Id.*

largest populations in the world. The ".cn" domain names are registered by the Chinese Internet Network Information Center ("CNNIC"), which also functions as an arbiter in disputes involving ".cn" names.[75] This process could make it easier for Chinese companies to settle their disputes since they are working under Chinese law and arbiters. The arbitration process operates much like the WIPO arbitration process. Given the current amount of internet usage, one would expect China to have a law or provision similar to the ACPA to prevent cybersquatters from operating in the country and taking over the domain names of many multi-national corporations. This is not the case however, as China largely relies on its own trademark and unfair use laws to protect against cybersquatters. China does allow for some differences in the way domain names are registered to try and keep cybersquatters away. All domain names registered in China must be approved by the Ministry Information Industry which administers domain names in the country.[76] This makes it easier to exclude cybersquatters from registering trademarked names or other names that are confusingly similar to trademarked names. The United States does not take such precautions and allows anybody to register any name they want which can lead to conflicts with domain names that need to be resolved in court through the ACPA or alternative dispute resolution under the UDRP.

With the emergence of the internet in China, "[a] number of international companies from Dupont to IBM, from Walt Disney to Proctor & Gamble have rushed to China trying to protect their precious intangible property from being usurped by

[75] China Internet Network Information Center, CNNIC Domain Name Dispute Resolution policy (2006), http://www.cnnic.net.cn/html/Dir/2006/02/14/4008.htm.
[76] China Internet Network Information Center, China Domain Name Regulations (2006), http://www.cnnic.net.cn/html/Dir/2005/03/24/2861.htm.

cybersquatters."[77] If the domain names that the companies are trying to protect end in ".cn," they can use the arbitration process discussed above, or they can try to resolve their disputes through the Chinese judicial system. The Chinese judicial system does not provide for any specific cybersquatting law, but relies on Chinese trademark, civil law, and laws against unfair competition.[78] Under these laws there are three remedies which include "(1) cancellation of the defendant's domain names; (2) transfer of the defendant's domain name registration to the plaintiff; and (3) compensation for the plaintiff's losses."[79] This is similar to the way in which issues are handled in the United States, except the United States is able to apply its specific cybersquatting law, the ACPA, which is better equipped to handle such disputes because of the reasons discussed earlier.

Another Asian country that has taken notice of the problems with cybersquatting on a smaller scale is Thailand. Thailand currently has over 8.4 million internet users.[80] Although the country has yet to try a cybersquatting case, it is questionable whether the country is equipped to deal with such issues, like many other smaller nations. Because §134 of the Thai Civil Procedure Code forbids the court from declining to listen to a case by alleging that there are no regulations which apply, the court, under §4 of the Thai Code, will apply a associated law of cases similar in nature, which will most likely have to do with trademark law.[81] Thailand, as well as the rest of the world, should have the

[77] Xue Hong, *Domain Dispute Resolution in China: A Comprehensive Review*, 18 Temp. Int'l & Comp. L.J. 1, 8 (2004) (discussing the size of China's market China in terms of drawing top companies from around the world who want to be involved in China's economic growth).
[78] *Id.* at 9 (noting that these laws have a long way to go in terms of dealing with specific cybersquatting disputes).
[79] *Id*. at 18.
[80] Central Intelligence Agency, The World Fact Book 2007- Thailand, https://www.cia.gov/library/publications/the-world-factbook/geos/th.html, (last visited November, 5, 2007).
[81] Areeya Ratanayu, *Cybersquatting in Thailand: The Thai Trademark Act and the Uniform Domain Name Dispute Resolution Policy*, 1 BUFF. INTELL. PROP. L.J. 203, 213 (2002).

responsibility of protecting their own people by using laws similar to the ACPA so that they do not have to rely on outside sources such as the UDRP to solve problems within their own country. Although Thai law may solve some cases, it would be much more efficient to utilize a specific cybersquatting law to make sure all disputes can be solved.

One country that has taken action and adopted a law similar to the ACPA is Japan, who boasts the third largest internet user population behind the United States and China with over 87.54 million users.[82] Japan has not adopted a specific provision within its laws that pertains to cybersquatting per se, but it has decided to broaden the scope of its original trademark laws so that it can apply to the registration of domain names.[83] This might not have been the best idea when a specific cybersquatting provision could have been adopted and in turn apply specifically to what it was enacted for, eliminating cybersquatters. In June 2001, the Japanese approved cybersquatting legislation to amend the Unfair Competition Prevention Law ("UCPL") to protect a trademark holder's right to domain names.[84] This was a big step for the country, as well as for the rest of the world, to show that the United States is not the only country that has the power and the insight to prevent cybersquatting within their borders by using the rules and laws of their own country.

In Japan, domain names are registered through the non-profit Japan Registry Services Company ("JPRS") and are limited to registering domain names ending in

[82] Central Intelligence Agency, The World Fact Book 2007- Japan, https://www.cia.gov/library/publications/the-world-factbook/geos/ja.html, (last visited November, 5, 2007).
[83] Brent Yonehara, *Landoftherisingsun.co.jp*: *A Review of Japan's Protection of Domain Names Against Cybersquatting*, 43 IDEA 207, (2003).
[84] *Id*. at 209.

".jp."[85] This limits the control that Japan has in regulating and registering domain names since they only have to worry about domain names specific to the Japanese market. There are two types of domain names in Japan; general use domain names ending in ".jp" which have very few restrictions and can be registered by any individual or corporation for either commercial or non commercial use, and organizational domain names which end in ".co.jp" or ".ne.jp," and are more heavily restricted in use and who may register the names.[86] For instance, only Japanese residents or companies domiciled in Japan may submit an application for a domain name, which is sometimes called the presence requirement. "The implication of this requirement is that foreign companies must set up Japanese subsidiaries, or maintain Japanese branch offices in order to submit an application for a domain name."[87] This policy helps Japan lure foreign companies to the country. The more companies that come and want domain names, the more business and economic growth the country can have.

The second requirement is that, "the domain name must be used within one year in Japan. The requirement was meant to prevent mass "warehousing" of domain names by hijackers."[88] Third, "the JPRS will only approve one domain name per registrant. This one domain per registrant policy is most obviously meant to deter would be cybersquatters from registering domain names en masse."[89] These three requirements are meant to reduce the amount of cybersquatting. These requirements seem to be a good

[85] *Id.* at 216.
[86] *Id.* at 219 (noting that this is a policy that could be applied in the U.S. registration of all domain names as it would regulate who may register which names. The result would be less domain name disputes that have to be settled through UDRP or litigation).
[87] *Id*. at 219.
[88] *Id.* at 220 (noting that this is another good requirement to prevent cybersquatting).
[89] *Id.* at 220 (noting that these policies should be looked at by the rest of the world when registering domain names to help prevent cybersquatting).

way of limiting the domain names and thus limiting cybersquatting. The United States might want to consider adopting similar procedures in order to protect individuals from cybersquatters. Also, with these policies in place, it would limit the amount of domain name disputes since not as many domain names would be registered on a regular basis. However it should be noted that the Japanese policy does not stop cybersquatters from registering very similar sounding company names. It would be a good idea to allow registrants of domain names the ability to register one name as well as similar misspellings of their domain name to further limit disputes.

The ACPA of the United States and the amendment to the UCPL in Japanese law have many similarities but they also have a few significant differences. For instance the amendment to the UCPL fails to include a provision for the transfer of the confusingly similar domain name to the legitimate trademark holder. "As a result, a plaintiff can sue to terminate an infringing use of a domain name but cannot actually recover the domain name from the defendant."[90] Also the amendment to the UCPL provides no factors that would determine what constitutes bad faith when using a domain name, whereas in the ACPA, the court has nine factors in which to consider when determining if a domain name was used in bad faith. "The rationale behind Japan's codification of "bad faith" seems to be that because bad faith is highly interpretive, leaving its determination to Japanese judges may create bad judicial rulings based on the judge's own predilections."[91] This provision helps to keep a judge's personal predisposition out of judgments and makes for a more generic judgment in which everybody can be judged the same. Also the ACPA has an *in rem* provision which allows United States companies to

[90] *Id.* at 222
[91] *Id.* at 223.

bring suit against foreign individuals or companies. The Japanese counterpart provides no such provision which results in only disputes between Japanese companies getting resolved and those involving a foreign party having to find an alternative method of dispute resolution.[92] This is not good for companies doing business in Japan and should be corrected in the future so that Japanese countries don't have to rely on outside sources for resolving domain name disputes. Although it is good that another country took the initiative to create laws pertaining to cybersquatting, the Japanese counterpart to the ACPA pales in comparison. It leaves certain disputes unresolved in which the parties will have to seek an alternative method to get their problems solved, such as alternative dispute resolution through UDRP with WIPO or one of the other dispute resolution agencies.

Until 2001, Japan adhered to ICANN and the UDRP for Japanese based domain name disputes, but has since developed its own similar dispute resolution process under the Japanese Arbitration Center for Intellectual Property ("JACIP"), which is authorized by the Japan Network Information Center ("JPNIC").[93] Japan having their own UDRP process could be beneficial because it will reduce the amount of cases that have to be heard by outside UDRP regulators such as WIPO. As stated before, the JACIP is similar to ICANN's UDRP except that JACIP would only be limited to disputes involving Japanese domain name registrants. It is clear that Japan is a front runner along with the United States in the fight against cybersquatting, but it is up to the rest of the world to catch up so that everyone may be protected throughout every country in the future.

[92] *Id* at 223-224.
[93] *Id*. at 225.

The Future of Cybersquatting

In a recent article in Wired Magazine, Author Jacob Ogles suggests that cybersquatting is evolving with the times. Instead of registering a domain name with hopes of profiting off of the name by people visiting a website, sensible domain name registrants have begun to register individual superstar domain names before the celebrity becomes popular. This is done with hopes of developing a work association with the new celebrity, offering to host a web site or create design work featuring the star.[94] These new breed of cybersquatters disagree with being tagged with the cybersquatter label, claiming that they intend no harm.[95] "In fact, some insist that they are doing good by protecting pre-celebrities from real cybersquatters out to make a quick buck."[96] These new cybersquatters may not intend any harm, but it doesn't mean that they will not cause harm by registering domain names that they have no rights in. On the other hand, the new cybersquatters may in fact be helping people out by hosting a website for their clients without the clients having to go find somebody else to host the site. Overall many individuals are registering the domains of amateur athletes, musicians and other potential celebrities anticipating that some of the names will become popular.[97] It is not hard to find out if certain domain names exist of an athlete or celebrity. Simply check the Whois database to see if their domain name is taken yet and by whom.[98] Often times companies come to the athletes and offer to host their sites for free with hopes of creating and

[94] Jacob Ogles, *Cybersquatters Try New Tactics* (2006), http://www.wired.com/news/technology/internet/0,70475-0.html (last visited on October 1, 2006).
[95] *Id.*
[96] *Id.* (emphasis omitted).
[97] *Id.*
[98] Who Is? Identity For Everyone, www.whois.com.

maintaining a business relationship.[99] Offering to host a celebrity domain name after the person becomes famous is a good idea in terms of making money, because as we have seen from case law and WIPO decisions, the odds of a cybersquatter actually hanging on to a domain name are not very good. One of the successful new form of cybersquatter bought the name of former American Idol participant William Hung soon after his awful "She Bangs" cover was aired.[100] He decided to offer Hung's parents partial ownership of the website while he maintained it for them. The cybersquatter claimed to be making a significant income, off the site which eventually became William Hung's official fan page.[101] Although it can be argued that this was not cybersquatting, it has just taken a different form. These new cybersquatters are still trying to make a profit off of other people's celebrity and names. Whether it is in bad faith is debatable as we cannot tell the true intentions of everyone. Overall, this is a for profit business however cybersquatting should not be relied upon for a full income, only to make a few quick bucks. If cybersquatters were donating their services or giving away the domain names for free, then we would really know they are registering the names out of the kindness of their hearts and not doing anything in bad faith.

Of course there are still cybersquatters out there who are relying on making a profit just from registering the domain name of a famous person and then selling it back to that person. With the political midterm elections recently concluded, the focus will be on the presidential elections in 2008, and cybersquatters have taken notice. Cybersquatters have registered a plethora of domain names belonging to the likes of

[99] *Id*.
[100] *Id.* William Hung has toured the world and has a cult following thanks to his American Idol Celebrity which he obtained from his dreadful performance.
[101] *Id*.

Hillary Clinton, Rudy Giuliani, John McCain and Barack Obama.[102] Some of these domain names have been registered since 1999 in anticipation of potential presidential runs.[103] One cybersquatter owning the rights to a Hillary Clinton domain name hopes to sell it for upwards of $30,000, while another cybersquatter will deal for a position on Clinton's campaign committee.[104] Clinton has already won the rights to a domain name using a UDRP hearing, and it is expected that others will soon fight for the right to use their own names.[105] Because many of these domain names will feature protected first amendment political speech it might be harder to obtain a domain name if it cannot be proven that a cybersquatter is using the website in bad faith for profit. It can be predicted that most candidates will be successful in obtaining these domain names because the majority of cybersquatters are out to make a quick buck from selling the domain names back to the candidates which would be considered bad faith. As the presidential elections draw near, and the candidates become clearer, many of these cybersquatters will realize that their efforts will go without reward, while others, if they can prove they were only using the domain name for political speech, may be in line to make a pretty penny, although $30,000 is extreme. It should also be noted that the more the domain name differs from the candidates name, the harder it will be for the candidate to obtain that

---

[102] Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, N.Y. Times, (November 18, 2006), http://www.nytimes.com/2006/11/18/us/politics/18domain.html?_r=2&oref=slogin&oref=slogin, (last visited on November 25, 2006).

[103] *Id*. The domain names that have been registered include, obama2008.org, hillary2008.com, barackobama2008.com, rudyforpresident.com, mccaingiuliani.com, clintongore2008.com, hillandbill2008.com, hillaryforpresident.com, mccain4president.com, barackobama.com, and obama2010.com.

[104] *Id.* It is unlikely that Clinton will offer a position in her campaign committee if she decides to run for president. She has already been successful in transferring a domain name bearing her name, so she will probably try and do that again if possible.

[105] *Id.* Clinton was successful in obtaining the domain name hillaryclinton.com from an Italian woman who had registered it in October 2001. Clinton used the UDRP process with the National Arbitration Forum.

domain name.[106] It will be harder to obtain a domain name if the general public does not associate that domain name with the person trying to obtain it. There must be some sort of secondary meaning involved. This could cause some of the candidates to be unable to obtain certain domain names that are more obscure and vary from their own name.

Conclusion

After analyzing the cybersquatting laws in the United States as well as some of the laws from around the world as well as the UDRP, it is clear that the United States is the frontrunner in the battle against cybersquatters, but that other countries are not that far behind in the development of similar laws. After analyzing the cases that utilize these laws, it is evident that there is a need for a general uniform cybersquatting rule or law that every country should have to abide by. This would prevent chaos and jurisdictional issues from interfering in disputes over domain names. A general rule would also make things easier when countries and corporations have to deal with foreign defendants, whom they may or may not have jurisdiction over in their country. A general rule would ensure that everyone is protected and that the same rules would apply to all. In the meantime, the United States has laid the groundwork for other countries to follow so that they can make their own cybersquatting provisions in the future. Furthermore, it is also fair to say that the closest thing we have to a universal rule is to bring cases before a UDRP panel. This might be the best way for multi-national corporations to get jurisdiction over foreign defendants so that they can protect their trademarks. It is also a cheaper and faster process, which is why I believe in the future almost all disputes will be decided under the UDRP rather than going to court. The court process will be used as an

[106] *Id*.

appeals process if the loser of a UDRP proceeding did not like the outcome of the ruling and they are able to get personal jurisdiction over a defendant. Also, court proceedings will be used if a plaintiff is seeking monetary compensation for the infringement. Individuals and celebrities will also continue to utilize the UDRP to protect their name or trademarks for the same advantages of saving time and money that the corporations will utilize the UDRP. In the long run, I believe that cybersquatters will always be lurking around, but they will be smarter about the way they approach obtaining the domain names of the trademarks they are infringing. Since most court and UDRP decisions favor plaintiffs who have trademarks, the cybersquatters have to evolve and adapt their way of thinking. This is already beginning to occur with the cybersquatters registering domain names of amateur athletes in the hopes that they become big stars so that they can capitalize on their success and hope to offer them a service of hosting a web page. The days are numbered of registering trademarked corporation names because case law has proven that it is very difficult for a defendant to win. It is now the time of a new era of regulation on the information super highway that is being led by the United States. It is now just a matter of time before the rest of the world follows suit.