

THE UDRP AND THE ACPA: WHAT ARE THEY, AND WHICH SHOULD BE USED?

Ryan Shewchuk

This essay compares the Uniform Domain-Name Dispute-Resolution Process (UDRP) and the Anticybersquatting Consumer Protection Act (ACPA.) These are two different avenues available to complainants looking to enforce their rights against so-called "cybersquatters." "Cybersquatter" most often refers to those who register domain names in bad faith, only to sell them to people who would be most interested in having the addresses. This leaves people who hold trademark or famous names that are the subject of the domain names three options. They can do nothing, simply letting the offending domain names continue to operate. Alternatively, they could pay off the cybersquatters, thus regaining control of the disrupted domain names. The third option is to fight to get the domain name back. In order to do this one of two processes is generally engaged, these being the UDRP and the ACPA.

The UDRP is a settlement process designed by the Internet Corporation for Assigned Names and Numbers (ICANN), and is part of the registration agreement for all <.com>, <.net>, and <.org> domain names. It involves the use of one of four stipulated dispute resolution providers to arbitrate the dispute between the parties and come up with a binding decision. The ACPA is part of the intellectual property law of the United States (US), and involves a civil court action engaging the US federal court system. The question that arises is: which process should I recommend for my client? The answer lies in the examination and comparison of both of these processes to determine what the strengths and weaknesses of each method are. While the UDRP is a quick and inexpensive process that is attractive to many complainants who simply seek possession of the domain name in question, the ACPA is a binding decision of the US courts which offers the possibility of compensation, not found in the UDRP, to victims of cybersquatting. Therefore, the remedy that is sought by the client and the amount of time and money the client is willing to invest in a resolution is relevant. It may also depend upon the type of question as to which forum would be best equipped to deal with the issues involved.

It is possible to engage both forums simultaneously in order to attain the best outcome. The UDRP can be used to gain control of the domain name quickly and economically, while the ACPA can be used to receive damages and finality to the conflict.

The proposed solution to the problem of cybersquatting is to increase regulation at the source of the problem – registration of the domain names.

* Faculty of Law, University of Manitoba (LL.B. 2002); Articling Student, Macleod Dixon LLP (Calgary).

I. INTRODUCTION

IN ORDER TO ANALYSE DOMAIN NAME DISPUTES, we must first look at the nature of domain names which are user-friendly forms of internet addresses.¹ The domain name system (DNS) translates internet protocol (IP) numbers (the four sets of numbers separated by decimals that identify every computer on the internet), into recognizable names. Generally, domain names break down into three parts: the server name (usually the world-wide web (www)), the second level domain (essentially the domain name), and then the top level domain (TLD), such as <.com>. When someone registers a domain name they are essentially picking a second level domain and a TLD. There are currently seven general TLDs (gTLDs) available for use on the internet, including <.com>, <.net>, <.org>, <.gov>, <.int>, <.edu>, and <.cc>.⁴ Each of the gTLDs are designed for a specific purpose. The most general and most popular of these are <.com>, <.net>, and <.org>, referring to the purposes of commerce, networks, and organizations respectively, although these three gTLDs are seen as non-exclusive. The other gTLDs are generally reserved for more specific purposes. Although <.com> is reserved for commercial activity it is seen, along with <.net> and <.org> as a catchall for those websites that do not possess any of the special attributes of the other TLDs.⁵ Of the 36 million domain names registered as of 27 July 2001, 22 million were of the <.com> variety.⁶ This paper will focus on domain name disputes involving the <.com>, <.net>, and <.org> gTLDs.

While many of the various country code TLDs (ccTLDs) are administered by national governments, universities, or private organizations, the

¹ O. R. Gutierrez, "Get Off My URL! Congress Outlaws Cybersquatting in the Wild West of the Internet" (2000) 17 Santa Clara Computer and High Tech. L. J. 139 at 145.

² J. M. Osborn, "Effective And Complimentary Solutions to Domain Name Disputes: ICANN's Uniform Domain Name Dispute Resolution Process and the Federal Anticybersquatting Consumer Protection Act of 1999" (2000) 76 Notre Dame L.R. 209 at 213.

³ Gutierrez, *supra* note 1 at 146.

⁴ <.cc> refers to the various two letter country codes assigned by the United Nations (for example <.ca> is assigned to Canada). On 16 November 2000 the Internet Corporation for Assigned Names and Numbers (ICANN) approved seven new gTLDs, and the plans to implement these new suffixes. See ICANN, online: <<http://www.icann.org/tlds/>>.

⁵ *Intermatic, Inc. v. Toepfen*, 947 F. Supp. 1227 at 1231 (1996).

⁶ See, Netnames, online: <http://www.netnames.com>.

gTLDs are administered by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit corporation that was set up in October of 1998 to deal with (among other things) the DNS, which was previously dealt with by the United States (US) government.⁷ Essentially ICANN oversees the administration of the gTLDs by accrediting companies to take registrations for domain names.⁸

Registering a domain name is a relatively easy process. The ICANN website has a page linking over 80 different companies that have been accredited thus far to register domain names, and a list of companies in the process of being accredited.⁹ By linking to any of these registrars, a simple process is followed and within 15 minutes (and with \$35) one could easily register a domain name for one year.

For example, I visited <register.com> to look into registering <ryan-shewchuk.com>. This website used a simple six-step process, taking approximately ten minutes. The first step involves picking a second level domain and a TLD. The registrar then completes a quick search to see if the name is already taken. Upon confirmation of the intent to register, you are required to log in by creating a user name and password. After logging in, you are prompted to fill in accurate information such as full name, address, and phone number, and then you must review that information for its accuracy. Finally, you must determine the length of term you desire (up to ten years). Payment then follows.

As can be seen, it is quite easy to register a domain name. The domain names are registered on a first come, first served basis. Thus the first person to offer up \$35 per year could obtain any unoccupied name. This is one of the sources of conflict for domain names. No one possesses a reserved right to any domain name and, although the registrar may include a disclaimer that it makes no representations that because a name is available it does not infringe a copyright or trademark, the registrars will nonetheless register any available name.¹⁰ Using this logic the

⁷ "About ICANN," online: ICANN <<http://www.icann.org/general/abouticann.htm>>.

⁸ Formerly there was a monopoly on domain registration for the <.com>, <.net> and <.org> held by Network Solutions Inc. (NSI) under an agreement with the National Science Federation (NSF). Since the inception of ICANN, and a subsequent reworking of the deal between NSF and NSI, competition has been introduced into the provision of registration services. NSI still maintains the database of all registered domain names.

⁹ "List of Accredited and Accreditation-Qualified Registrars," online: ICANN <<http://www.icann.org/registrars/accredited-list.html>>.

¹⁰ This open policy of registration only applies to the general gTLDs, and certain ccTLDs that have been opened to the world for various reasons. See Register.com, online: <<http://www.register.com>> for a list of the TLDs that can be registered by this process.

average person could register <microsoft.com> if it weren't already registered. The ease and low cost of registration gives rise to the problem of cybersquatting.

Cybersquatting refers to individuals who:

attempt to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing the goodwill of the trademark.¹¹

Simply put, individuals register domain names before trademark holders get around to reserving these names, and then try to turn a profit by selling the domain names back to the trademark holders. This definition has been expanded to include cases where people register the domain names of their competitors in order to disrupt the competitor's business.¹² Cybersquatting also refers to registered domain names that are similar, or misspelled concoctions of famous or trademarked names, used to cash in on internet users that make typographical errors while entering domain names.¹³

Cybersquatters can generate a profit through various means by possessing famous domain names. The first involves using the sites to host advertisers, which link off of that site. People are drawn to the famous website looking for a specific purpose and may end up clicking on a banner advertisement of a sponsor to the site. Advertisers pay the website owner for each click. Another way cybersquatters may use these sites to make money is by linking the famous domain name to other sites, which generate advertising revenue as well. In this case the user types in the famous name looking for a certain web page and instead is transported to an unrelated page, usually featuring pornography.¹⁴ A final way in which cybersquatters attempt to profit, which has already been mentioned, is by selling the famous domain name back to trademark holders, often for sums far in excess of the initial cost of registration.

Aggrieved trademark holders, as well as those with service marks or otherwise recognizable names, are thus left with a number of options. They can simply register a domain name that is not a precise replica of

¹¹ *Supra* note 5 at 1233.

¹² M. Mueller, "Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy," online: Convergence Center: Syracuse University <<http://dcc.syr.edu/roughjustice.htm>>.

¹³ *Ibid.*

¹⁴ *Ibid.*

their famous name, and attempt to carry on business. Another option is simply to pay off cybersquatters, an option that may be cheaper and easier than engaging in a dispute resolution process to get the name back. However, these options are not always available as, for example, in cases where cybersquatters demand exorbitant amounts of money for the domain name or in situations where the cybersquatter has registered many or all of the reasonably similar domain names to the domain name in issue, thus frustrating the trademark holder's attempt to register a recognizable domain name. Clearly something needed to be done as trademark law at the time was not designed to deal with domain name trademark issues, and the Network Solutions, Inc. (NSI) dispute resolution policy was seen as inadequate.¹⁵

The end of 1999 saw the introduction of two new regimes designed to combat cybersquatters. On 26 August 1999, ICANN adopted the Uniform Domain-Name Dispute-Resolution Policy (UDRP) and implemented this process on 24 October 1999.¹⁶ All registrars accredited by ICANN must adopt the UDRP and include it in the registration agreements that they offer. The US congress was not blind to the problem of cybersquatting either, and subsequently passed the Anticybersquatting Consumer Protection Act (ACPA) as an amendment to the current Trademark Act of 1946.¹⁷ The ACPA came into force on 29 November 1999.¹⁸

II. THE UDRP

UNDER THE UDRP, a domain name holder must submit to a mandatory administrative proceeding whereby a complainant asserts to any approved resolution provider¹⁹ the following grounds in accordance with the Rules for Uniform Domain Dispute Resolution Policy (Rules of Procedure) that:²⁰

¹⁵ The analysis of past domain name resolution processes falls outside of the scope of this essay. For further analysis of this issue consult K. Eng, "Breaking Through The Looking Glass: An Analysis Of Trademark Rights In Domain Names Across Top Level Domains" (2000) 6 Boston U.J. of Science and Tech. L. 7.

¹⁶ "Uniform Domain Name Dispute Resolution Policy," online: ICANN <<http://www.icann.org/udrp/udrp-policy-24oct99.htm>>.

¹⁷ Also known as the *Lanham Act*. 15 U.S.C.A. § 1125(d) (2000).

¹⁸ C. F. Schulte, "The New Anticybersquatting Law and Uniform Dispute Resolution Policy for Domain Names" (2000) 36 Tort and Insurance L. J. 101 at 109.

¹⁹ "Approved Providers For Uniform Domain Name Dispute Resolution Policy," online: ICANN <<http://www.icann.org/udrp/approved-providers.htm>>.

²⁰ "Rules For Uniform Domain Name Dispute Resolution Policy," online: ICANN <<http://www.icann.org/udrp/udrp-rules-24oct99.htm>>.

- i. [the] domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
- ii. [the domain name holder possesses] no rights or legitimate interests in respect of the domain name; and
- iii. [the] domain name has been registered and is being used in bad faith.²¹

Note that it is up to the complainant to prove the existence of all three elements.²²

The first element requires that the domain name be identical or confusingly similar to a trade or service mark. Thus in order to bring a claim under the UDRP, one must be a trademark or service mark holder. This strict provision has been interpreted more generally to favour famous names such as Julia Roberts as well, stating that "the name 'Julia Roberts' has sufficient secondary association with [the] Complainant that common law trademark rights do exist under US trademark law."²³ Thus, for easily recognizable names such as Julia Roberts, Bruce Springsteen, and Celine Dion, the fact that the name is so widely recognizable establishes common law rights to the name.²⁴ The principle of the aforementioned cases has not stretched to famous names such as "Sting," used by the popular entertainer, because the word "sting" is also a common word in the English language, with a number of different meanings, and thus it was found that Sting did not possess sufficient common law rights to that name.²⁵

The likeness of the domain name has also been interpreted at a more relaxed standard. When dealing with trademarks, capitalization and punctuation are important. However, domain names are not case sensitive. No spaces are allowed between characters, and the characters are limited to letters, numbers, and hyphens. In dealing with disputes over

²¹ *Supra* note 16 at para. 4(a).

²² *Ibid.*

²³ *Julia Fiona Roberts v. Russell Boyd*, WIPO D2000-0210 at 2, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

²⁴ *Celine Dion and Sony Music Entertainment (Canada) Inc. v. Jeff Burgar operating or carrying on business as Celine Dion Club*, WIPO D2000-1838 at 3 and *supra* note 23 at 2, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

²⁵ *Gordon Sumner, p/k/a Sting v. Michael Urvan*, WIPO D2000-0596, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

names such as Wal-Mart, the tribunals have accepted that <walmart.com> would be confusingly similar and that domain names are not identical to trademarks due largely to technical constraints of the DNS.²⁶

The second ground that a complainant has to prove is that the domain name holder possesses no rights or legitimate interests in the domain name. The UDRP also sets out a non-exhaustive list of defences to these allegations:

- i. [if] before any notice [of the dispute, the respondent used, or made] 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. [if the respondent] (as an individual, business, or other organization) [has] been commonly known by the domain name, even if the respondent holds no trademark or service mark rights; or
- iii. [if the respondent is] 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.²⁷

These defences are not exhaustive of the considerations that may be looked at by the tribunal. Each of the defences may be better analysed by looking into some of the decisions of the arbitration panels.

The first defence relates to a situation in which the domain name holder used or was preparing to use the website for bona fide purposes prior to notice of the dispute. One could contemplate a case where the domain name holder is quite unaware of the similarity to a trademark, and is legitimately prepared to use the website for commercial purposes of his own design, not to disrupt the business of competitors, nor sell the name for profit.

Such a case arose in *Sealstore.com LC. v. Sealpool Limited*, in which a dispute over the domain name <sealstore.com> arose. The respondent Sealpool Limited had made legitimate preparations to sell industrial seal products online and had registered <sealstore.com>, <sealshop.com>,

²⁶ *Wal-Mart Stores, Inc. v. Walsucks and Walmarket Puerto Rico*, WIPO D2000-0477 at 10, online: WIPO Arbitration and Mediation Center <<http://arbitrator.wipo.int/domains/decisions/index-gtld.html>>.

²⁷ *Supra* note 16 at para. 4(c).

and <sealmart.com> in order to obtain the most accessible name.²⁸ There had been extensive preparation on the part of the respondent for further market study to determine which domain name ought to be used to market the product online. Due to this extensive preparation, the complainant failed to prove its claim despite the fact the domain name was identical to or confusingly similar to a trade name.

The second enumerated defence contemplates a case where, although the domain name holder does not have a trademark for the domain name, he has been known by that name prior to the dispute arising. This would cover cases where the domain name in dispute is so common that someone could become known by that name, regardless of trademarks that may exist for that particular name. One could easily conceive of cases where various abbreviations, slang terms, or acronyms for a certain organization are used as a domain name, and it turns out that the particular domain name chosen happens to be identical or confusingly similar to that of a registered trademark holder. Such a case arose in *Avnet, Inc. v. Aviation Network, Inc.*, where the respondent was able to prove that it had been known by the name "Avnet" for at least ten years prior to its registration of the domain name <avnet.net>.²⁹

This principle was not extended in a case where the trademark holder claimed rights in a domain name that was a slang term used to refer to its well established trademark. The case was *Canadian Tire Corporation, Limited v. Mick McFadden* in a dispute over the domain name <crappytire.com>³⁰. In this case the Canadian Tire Corporation tried to argue that "crappytire" was a commonly used slang term used to refer to Canadian Tire stores, and that therefore it should be able to hold common law rights to that term, despite the fact that this term was not one of the many trademarks that the complainant held regarding the Canadian Tire name. This argument was rejected in the panelists' decision.³¹

The third enumerated defence covers situations that involve fair use of the domain name in a legitimate noncommercial context, without the

²⁸ *Sealstore.com L.C. v. Sealpool Limited*, (2001) FA0101000096535, online: National Arbitration Forum <<http://www.arb-forum.com/domains/decisions/96535.htm>>.

²⁹ *Avnet, Inc. v. Aviation Network, Inc.*, WIPO D2000-0046 at 2, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

³⁰ WIPO D2001-0383, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>> (pagination unavailable).

³¹ *Ibid.*

intent to misleadingly divert customers or tarnish the trademark at issue. This defence protects criticism sites where the trade name may be part of the domain name but the intent is not commercial; rather it is to raise awareness or create a forum for activist activities. The arbiters under the UDRP have often looked to US trademark law to analyse parody cases.³² The view accepted in these cases is that it must be clear that a site is for parody. The simple adding of a "sucks" prefix to a trademark does not impute that the site is a criticism site. Rather the site itself must actually be used for criticism or parody.³³ This defence of legitimate noncommercial use should also protect fan sites, however arbitration panels have not always decided cases in this way. In the case of *Reg Vardy Plc. v. David Wilkinson* it was found that a complaint site constituted bad faith, as intent to disrupt the business of a competitor (a ground that will be discussed later).³⁴ The problem with the decision in this case is that the respondent was a disgruntled customer of the complainant car dealership, and not a competing dealership.

The aforementioned defences were intended to protect domain name holders that are not really cybersquatters. The UDRP has not always been interpreted properly in this fashion and the policy, as well as the arbitration panels that implement it, have been under steady criticism for decisions that seem inconsistent with a plain reading of the UDRP.³⁵

There is one more element that the complainant must prove in a UDRP case – the element of bad faith. The UDRP has enumerated some of the grounds that might give rise to bad faith:

- i. [if there are] 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 ... 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 costs related to the domain name; or
- ii. you have registered the domain name in order to prevent

³² *Supra* note 26 at 10.

³³ *Ibid.*

³⁴ WIPO D2001-0593, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>> (pagination unavailable).

³⁵ For a more thorough analysis of this see: I. L. Stewart, "The Best Laid Plans: How Unrestrained Arbitration Decisions Have Corrupted the Uniform Domain Name Dispute Resolution Policy" (2001) 53 Federal Communications L. J. 509.

the owner of the trademark ... 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 the website, or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your website ... or of a product ... on your website or location.³⁶

Proving bad faith is the essence of most proceedings. The grounds listed in the UDRP are not exhaustive. Rather these grounds essentially outline what has been defined earlier as cybersquatting.

It is also important to note that the domain name must be registered and used in bad faith. This requirement of use has been side-stepped by the argument that holding a domain name for resale constitutes commercial use. For example, in the first case decided under the UDRP, although the respondent had not actually put the website in dispute to bad faith use, the mere holding of the domain name for sale was seen to constitute commercial use.³⁷

The first bad faith ground is descriptive of the classic case of cybersquatting, where a domain name is registered for the sole purpose of resale for substantially more than it costs to register it. It is important to remember that it is quite easy to register a domain name at a cost of only \$70 for a two-year registration period. Offering to sell the domain name for as little as \$1,000 may constitute bad faith.³⁸ The determination of bad faith does leave room however, for cases where there has been considerable work done in connection with the domain name, but the domain name holder is offering to sell it to the trademark holder at a reasonable price.

The next listed circumstance of bad faith has to do with registering a domain name to prevent the owner of the trademark from reflecting his mark in the domain name, provided that there is a pattern of such conduct. This element may also serve to help strengthen or disprove other

³⁶ *Supra* note 16 at para. 4(b).

³⁷ *World Wrestling Federation Entertainment, Inc. v. Michael Bosman*, WIPO D99-0001 at 4, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

³⁸ *Ibid.*

defences, such as use of a domain name as a criticism or parody site.³⁹ It was often the case that cybersquatters would register tens or hundreds of domain names. In a US trademark case pre-dating the UDRP, Dennis Toeppen, a noted cybersquatter, had registered approximately 240 domain names that incorporated well known business names, notably <ussteel.com>, <deltaairlines.com>, <britishairways.com>, <crateandbarrel.com>, and <eddiebauer.com>.⁴⁰

Other indicia of bad faith cover areas of registering a domain name to disrupt the business of a competitor, and using the domain name to attract people to a website or other online location for commercial gain, while playing on their mistake as to the connection to the complainant's mark or famous name. Two cases contrast the second of these enumerated bad faith grounds. In *Bruce Springsteen v. Jeff Burgar and Bruce Springsteen Club*, a dispute over <brucespringsteen.net>, the claimant failed to prove that there was a bad faith attempt to lure internet users to another website, notably <celebrity1000.com>. The arbiter found that a search for "Bruce Springsteen" through a search engine would produce many hundreds of hits, not all of which were official sites. Thus a reasonably educated internet browser would quickly realize that the site maintained by the respondent was not an official site, and could therefore move on to other search results.⁴¹

A different outcome was reached in the case of *Madonna Ciccone p/k/a Madonna v. Dan Parisi and "Madonna.com."* In that case, it was found that the respondent was using the <madonna.com> site to host pornographic materials, and was attempting to lure internet users based on the "Madonna" name. It was irrelevant in this case that singer/songwriter Madonna had erotic materials published elsewhere as the respondent was trying to infer that the images on his site were somehow connected to the "Madonna" name.⁴² There was no discussion in the *Madonna* case regarding the internet user's legitimate expectation of finding information on the singer at the site, simply because the name was <Madonna.com>.

³⁹ *Supra* note 26 at 12.

⁴⁰ *Supra* note 5 at 1230.

⁴¹ *Bruce Springsteen v. Jeff Burgar and Bruce Springsteen Club*, WIPO D2000-1532 at 3, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

⁴² *Madonna Ciccone, p/k/a Madonna v. Dan Parisi and "Madonna.com,"* WIPO D2000-0847 at 3, online: WIPO Arbitration and Mediation Center <<http://arbiter.wipo.int/domains/decisions/index-gtld.html>>.

III. THE ACPA

THE INTENT OF THE ACPA is also to combat cybersquatters by adding new provisions to existing trademark law. The ACPA was brought into force around the same time as the UDRP, despite debate as to whether the ACPA would undermine the UDRP.⁴³ The requirements to prove cybersquatting are essentially the same under the ACPA as under the UDRP, however, as will be discussed later, there are major differences relating to procedure and remedies. In order to understand the ACPA and why it was enacted, a very brief analysis of the prior legislation and litigation to combat cybersquatting is necessary.

Prior to the ACPA, the only options available for trademark holders under US law were to sue the cybersquatter for trademark infringement or to seek a remedy under the Federal Trademark Dilution Act of 1995 (FTDA).⁴⁴ This litigation was costly and one could not be certain as to the outcome.⁴⁵ The problem when pursuing a cybersquatter for trademark infringement was that there needed to be proof of a likelihood of consumer confusion, while taking into account how closely related the goods and services of the two parties were.⁴⁶ Thus a plaintiff could only be successful if the domain name holder used the website for a commercial purpose that consumers might mistakenly believe was that of the trademark holder. This was a tough argument for trademark holders as the majority of cybersquatters did not use the domain names to offer competitive goods and services; rather they registered the domain names for the purpose of selling them to the trademark holders. The legal analysis of "likelihood of confusion" did not work for this type of cybersquatter.⁴⁷

Suing a cybersquatter under the FTDA was no easy task either. To be successful the trademark holder had to prove that the actions of the domain name holder were diluting the fame of the trademark. This law, while perhaps intended for use against cybersquatters,⁴⁸ really only protected those with famous trademarks. Thus a large burden was placed on the trademark holder to prove first that he held a famous mark, and second that the mark was being diluted by the actions of the domain name

⁴³ Osborn, *supra* note 2 at 228.

⁴⁴ 15 U.S.C.A. § 1125(c).

⁴⁵ *Sporty's Farm L.L.C. v. Sportman's Market, Inc.*, 53 U.S.P.Q. 2d 1570 at 1574 (2000).

⁴⁶ J. Voelzke, "New Cybersquatting Law Gives Trademark Owners Powerful New Weapons Against Domain Name Pirates" (2000) vol. 17, no. 2 Computer Lawyer 3.

⁴⁷ Gutierrez, *supra* note 1 at 155.

⁴⁸ *Ibid.* at 157.

holder.⁴⁹ Although the FTDA was stretched to its limits by the courts in order to catch the extreme cybersquatting cases, the courts were reluctant to find dilution where the defendant could not be found to have the intent to profit from selling the domain name to the trademark holder.⁵⁰ Cybersquatters had gotten more sophisticated and no longer offered the domain names for sale in a manner that could implicate them under federal dilution case law.⁵¹ The ACPA was thus enacted to remedy the shortcomings of the FTDA.⁵²

The ACPA provides for a civil action by the owner of a mark, (which includes a personal name) against a person who has a bad faith intent to profit from that mark, and who registers, traffics, or uses a domain name that is identical or confusingly similar to or dilutive of the mark.⁵³ The act also sets out what constitutes a famous name or trademark, and lists nine non-exhaustive grounds that a court may consider when looking at bad faith:

- 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 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 holder or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

⁴⁹ Voelzke, *supra* note 46 at 3.

⁵⁰ Gutierrez, *supra* note 1 at 158.

⁵¹ *Supra* note 45 at 495.

⁵² *Ibid.* at 496.

⁵³ *Supra* note 17 at (d)(1)(A).

- vii. the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;
- viii. the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and
- ix. the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous⁵⁴

It is notable that the first four grounds are similar to the defences of legitimate interest as enumerated in the UDRP. The other grounds lean more to proving of bad faith. It is also important to note that the ACPA also includes a safe harbour provision that states that bad faith will not be found where a court determines that the domain name holder "...believed and had reasonable grounds to believe that the use of the domain name was for fair use, or otherwise lawful."⁵⁵

The first two elements of bad faith go to determining if the domain name holder possesses any legitimate right to hold the domain name due to the name being reflective of his own name, a name that he is commonly identified by, or a name that he has intellectual property rights in. This would protect a situation where a domain name holder has registered a name that could legitimately describe his business. In the case of *Mattel, Inc. v. Internet Dimensions Inc.*, in a dispute over the domain name <barbiesplaypen.com>, the defendant testified that the "Barbie" name in the domain name referred to a girlfriend of his former partner in his adult website enterprise. The Court rejected this as a basis for a claim that he had a legitimate right to use the name "Barbie" to protect his pornographic site.⁵⁶ This type of argument, a weak attempt to provide some legitimate link to the domain name in question, was also rejected in the *Sporty's Farm* case.⁵⁷

⁵⁴ *Ibid.* at (d)(1)(B)(i).

⁵⁵ *Ibid.* at (d)(1)(B)(ii).

⁵⁶ *Mattel, Inc. v. Internet Dimensions*, 55 U.S.P.Q. 2d 1620 at 1624 (2000).

⁵⁷ *Supra* note 45 at 1577.

The third factor in establishing bad faith is to determine if the domain name holder has used the domain name for the bona fide offering of goods or services. Although in the *Mattel* case it was found that the defendant had registered the name to bona fide offer adult entertainment, bad faith was found on other grounds.⁵⁸ It is uncertain how much weight is to be placed on this ground. It is likely that it would only be beneficial to the defendant if he also had a reasonable claim to use the name in issue. For example, if there had been better evidence in the *Mattel* case that the defendant had a legitimate use of the domain name, such as his own name being "Barbie," the outcome may have been different.

The fourth element of bad faith goes to whether the domain name holder used the domain for bona fide noncommercial or fair use. This is similar to a provision found in the UDRP and deals with the subject of parody and criticism sites. In *Lucent Technologies, Inc. v. LucentSucks.com*, it was determined that if the defendant could prove that <lucentSucks.com> was a parody or criticism site, the plaintiff's case would be seriously weakened.⁵⁹ (The case was determined on a jurisdictional issue unrelated to the determination of bad faith.) In the case of *Shields v. Zuccarini*, the defendant was not entitled to a protest use defence because he had used the sites in question for commercial purposes until the plaintiff sued him.⁶⁰ In *People For The Ethical Treatment of Animals, Inc. v. Doughney (PETA)*, the defendant used the domain name <peta.org> for his nonexistent organization "People Eating Tasty Animals."⁶¹ The Court found that the domain name was used for commercial purposes due to the fact that there were several links from the website to commercial sites offering, among other things, the sale of leather goods and meat.⁶² Nonetheless, the Court commented on the use of parody sites. The Court found that "a parody exists when two anti-theoretical ideas appear at the same time," and since the site was only one sided, it was not covered by a parody defence.⁶³ This seems to be a very limiting view of the parody and criticism defence.

The fifth element used to determine bad faith involves a consideration as to whether the domain name holder's intent is to divert internet users

⁵⁸ *Supra* note 56 at 1625.

⁵⁹ *Lucent Technologies, Inc. v. LucentSucks.com*, 54 U.S.P.Q. 2d 1653 at 1659 (2000).

⁶⁰ *Shields v. Zuccarini*, 89 F. Supp. 2d 634 at 640 (2000).

⁶¹ *People For The Ethical Treatment of Animals, Inc. v. Doughney*, 113 F. Supp. 2d 915 at 918 (2000).

⁶² *Ibid.* at 918.

⁶³ *Ibid.* at 921.

to his website or other linked sites that could harm the goodwill represented by the mark. The purpose for doing so must be either for commercial gain or to tarnish the mark of the trademark holder by creating confusion as to the source, affiliation, or sponsorship of the site. This has been found in cases such as the *Mattel* case, where it was determined that the defendant was using the name "Barbie" to attract users to his adult site, and that the fact that the site contained adult content could tarnish the image of Mattel's Barbie products in the mind of consumers.⁶⁴ In the case of *Electronic Boutique Holdings Corp. v. Zuccarini*, the defendant registered a number of misspellings of the plaintiff's domain names in order to cash in on typographical errors by internet users trying to reach Electronic Boutique's website.⁶⁵ These domain names were for commercial use because when they were entered they effectively "mouse-trapped" the internet user by having several browser windows open at once, each advertising a product, and each advertiser paying Zuccarini per window opening.⁶⁶

The sixth enumerated ground upon which bad faith may be found relates to the efforts of the domain name holder to sell or transfer the domain name to the mark holder or third party for financial gain without having used the domain for bona fide offering of goods or services. This element allows for the legitimate transfer of a domain name from one person to another for financial gain, if the domain name holder legitimately used the domain name and was receiving a financial incentive to part with the domain name. In *Virtual Works, Inc. v. Volkswagen of America, Inc.*, the internet service providing business "Virtual Works" registered the domain name <vw.net> and used it as their website for approximately two years.⁶⁷ Virtual Works recognized the resemblance of the name but decided to use it anyhow, noting that should Volkswagen offer to buy it they could sell the name for a profit.⁶⁸ When Volkswagen inquired into purchasing the domain name from Virtual Works, it responded by threatening that if Volkswagen didn't make an offer within 24 hours, it would sell the domain name to the highest bidder. Thus, despite the fact that Virtual Works had carried on business under the <vw.net> domain name, it had

⁶⁴ *Supra* note 56 at 1624.

⁶⁵ *Electronic Boutiques Holdings Corp. v. Zuccarini*, (2000), online: Gigalaw <<http://www.gigalaw.com/library/electronicboutique-zuccarini-2000-10-30-pl.html>>.

⁶⁶ *Ibid.*

⁶⁷ *Virtual Works Inc. v. Volkswagen of America, Inc.*, 57 U.S.P.Q. 2d 1547 at 1548 (2001).

⁶⁸ *Ibid.* at 1549.

not registered the name solely for its resemblance to the company, but also because of its possible future value down the road. The Court found that because Virtual Works intended to profit from the sale of the domain name, it could not use the safe harbour provision of the ACPA.⁶⁹

The seventh ground listed under bad faith deals with domain name holders who provide false information when applying for registration of the domain name, or who intentionally fail to maintain accurate contact information. This situation, although not in itself evidence of cybersquatting, has occurred in two of the cases that have already been discussed in this paper. In *Mattel* the defendants registered the domain name with an address in Nevada, and after the filing of the complaint against them, changed the listed address to one located in Costa Rica.⁷⁰ It was determined that the defendants did not have a place of business at either of the provided addresses. The Court found that by giving false information the defendants had impeded the efforts of third parties in serving them with complaints.⁷¹ In *PETA* the defendant had registered the domain name as a non-profit organization named "People Eating Tasty Animals."⁷² No such organization existed. Thus, although giving false information was not determinative of cybersquatting, it was certainly an aggravating factor and was used to show bad faith on the part of the defendants.

The eighth ground listed under bad faith looks at the conduct of the domain name holder in regard to registering multiple domain names that he knew were identical or confusingly similar to well known marks. Note that, as prior conduct was also a factor in the analysis of the sixth and seventh grounds for determining bad faith, courts seem to place a lot of emphasis on the existence of prior bad behavior. For example, in *Mattel* the defendants had previously registered the domain names <clits-r-us.com> and <billgatesnude.com>. When approached by Toys 'R Us regarding trademark infringement the defendants had immediately stopped using the <clits-r-us.com> domain name.⁷³ In the *PETA* case it was found that both the plaintiff and the defendant had prior conduct involving the registration of domain names that were famous and/or were the subject of protest by the parties. The Court rejected the defendant's argument that the actions of the plaintiffs should preclude their action against his activities.⁷⁴

⁶⁹ *Ibid.* at 1549, 1551.

⁷⁰ *Supra* note 56 at 1625.

⁷¹ *Ibid.*

⁷² *Supra* note 61 at 918.

⁷³ *Supra* note 56 at 1625.

⁷⁴ *Supra* note 61 at 921.

The ninth enumerated ground for determining bad faith deals with an analysis of the extent to which the mark incorporated in the domain name registration is or is not distinctive and famous, as defined elsewhere in the act. This analysis was done in the *Mattel* case where it was found that the word "Barbie" was both distinctive and famous as a trademark of Mattel.⁷⁵

The nine grounds listed in the ACPA are not exhaustive of the factors that the court can assess in determining bad faith. Many courts look to a quote in *Sporty's Farms L.L.C. v. Sportman's Market, Inc.*, the first appellate level decision interpreting the ACPA, which opened the door for the remaining factors to be considered. In that case the Court stated that:

[t]he most important grounds for our holding that Sporty's Farm acted with a bad faith intent, however, are the unique circumstances of this case, which do not fit neatly into the specific factors enumerated by Congress but may nevertheless be considered under the statute.⁷⁶

This justifies the court looking at any factors its feels are relevant to the current dispute.

IV. A COMPARISON OF THE REGIMES

THE UDRP AND THE ACPA were both created with the intent of eliminating cybersquatting. The UDRP engages an alternative dispute resolution (ADR) regime, while the ACPA engages the US federal court system. There are advantages and disadvantages to each system; they should be examined based on what the client is seeking from the dispute resolution process. The main differences arise in the areas of time, cost, remedy, enforceability, and scope of judgment.

The first major difference between the regimes concerns the amount of time it takes to engage the process. The UDRP is designed to deliver judgments within 45 days of the initiation of the claim.⁷⁷ Ten days after the issuance of the judgment, allowing time to appeal the matter to the courts, the judgments are to be enforced. Thus the UDRP is designed to facilitate an end to the domain name dispute within two months of the initiation of the complaint. The ACPA, on the other hand, engages the court system. As the ACPA is a civil action, the process of resolution

⁷⁵ *Supra* note 56 at 1622.

⁷⁶ *Supra* note 45 at 1577.

⁷⁷ "FAQ," online: ICANN <<http://www.icann.org/general/faq1.htm>>.

moves at a slower pace than an ADR system as certain procedures are observed. Federal courts have taken anywhere from 49 to 202 days to render a preliminary injunction in cybersquatting cases.⁷⁸ Thus the UDRP definitely has an advantage when it comes to expediency and when the remedy that is sought is the cancellation or transfer of a domain name.

One of the largest differences between the two systems lies in available remedies. If one initiates a claim under the UDRP the only remedies available are the cancellation or transfer of the domain name. The ACPA, as federal trademark legislation, is capable of granting several remedies. Under the ACPA the range of remedies open to the plaintiff range from the cancellation or transfer of the domain name to an injunction and damages.⁷⁹ The plaintiff also has the option of choosing a special damages remedy where, instead of actual damages, the plaintiff, at the discretion of the court, may be awarded \$1,000 to \$100,000 per domain name.⁸⁰ The awarding of damages of a monetary value per domain name was recently upheld by an appellate level court.⁸¹ When damages are at issue the ACPA has a clear advantage.

One further issue relating to remedies concerns the power of the court, under the ACPA, to allow an *in rem* proceeding. If the plaintiff cannot reasonably locate the domain name holder, the plaintiff may be allowed to proceed in an action against the domain name itself based on the jurisdiction of the registrar with which the domain name was registered.⁸² Thus, as long as the domain name is registered with a US-based registrar, the plaintiff is not necessarily precluded from an action simply because the domain name holder cannot be located.⁸³ However, under *in rem* jurisdiction, the remedies of the court are limited to cancellation and transfer of the domain name.⁸⁴ If the domain name holder has used an alias to register the domain name, the ACPA gives some hope to the plaintiff. However, the UDRP helps sweep aside jurisdictional problems as it is binding on the parties involved regardless of the jurisdiction in which they reside (once the UDRP has been engaged by the complainant).

⁷⁸ Osborn, *supra* note 2 at 239.

⁷⁹ *Ibid.* at 236.

⁸⁰ 15 U.S.C.A. § 1117(d).

⁸¹ *Shields v. Zuccarini*, 59 U.S.P.Q. 2d 1207 at 1214 (2001).

⁸² *Supra* note 17 at (d)(2)(A).

⁸³ The NSI keeps a WHOIS database that contains the contact information for all websites that are registered. If this information is erroneous or incomplete, this may give rise to problems of locating the domain name holder, online: NSI <<http://www.networksolutions.com/cgi-bin/whois/whois>>.

⁸⁴ *Supra* note 17 at (d)(2)(D)(I).

Another factor to analyse is the cost involved in the different proceedings. Under the UDRP, the complainant chooses from one of four approved dispute resolution providers and then selects the size of panel desired, from one to three panelists.⁸⁵ The cost then ranges from \$750 - \$2,000 for a single panelist, and \$2,200 - \$4,500 for a three-person panel - the precise cost depending upon the number of domain names at issue.⁸⁶ In addition, most of the resolution providers enforce word limits on submissions, which significantly reduces legal fees.⁸⁷ On the other hand, while applications to the court may be cheaper under an ACPA lawsuit, as the procedure continues, legal fees may make the process very expensive.

An important issue under any dispute resolution scheme concerns the enforceability of the outcome. UDRP decisions, the cancellation or transfer of a domain name, are implemented by the registrars after a ten day appeal period has lapsed. Decisions reached by the arbitration panels under the UDRP are not binding on the courts, but the courts have declined to decide what the precise standard of review would be for the arbitration panel's decision, or what degree of deference would be owed to those decisions.⁸⁸ The decisions under the ACPA are decisions of the US Federal Court and, as such, are enforceable by courts in that jurisdiction. Although the decisions under both processes are subject to appeal, when a decision of the Federal Court is appealed, a high level of deference is given to the lower courts, especially relating to determinations of fact. The UDRP is not appealed to another arbitration board, but the policy allows for the disputes to be taken before courts of competent jurisdiction.⁸⁹ Thus, in a highly contested case, it may be beneficial to ignore the UDRP and initiate a claim under the ACPA, since there may be a significant likelihood that the decision of the panel under the UDRP is going to be appealed by initiating an ACPA proceeding anyhow, assuming there are no other jurisdictional issues.

The final major area of contrast between the two systems is that of the scope of judgment. This term is a "catchall" phrase to deal with various

⁸⁵ *Supra* note 19; *supra* note 20.

⁸⁶ To obtain the latest rates consult the various dispute providers listed, *supra* note 19.

⁸⁷ eResolutions is the exception; see online: eResolutions <<http://www.eresolution.ca>>. Also see C.D. Emerson, "Bad Faith in Cyberspace: Trademark Rights on the World Wide Web" (2000) 36 Tenn. Bar J. 14 at 16.

⁸⁸ *Weber-Stephen Products Co. v. Armitage Hardware and Bldg. Supply, Inc.*, 54 U.S.P.Q. 2d 1766 at 1767 (2000).

⁸⁹ *Supra* note 16 at para. 4(k).

procedural and practical considerations. The first of these relates to the use of precedent. Although the doctrine of precedent is firmly established in US courts, it is uncertain whether panelists under the UDRP are bound by prior decisions. From an analysis of some decisions from the UDRP dispute resolution providers (DRPs), there is some evidence of panelists referring to prior decisions of both arbitration panelists and US courts, but there is no evidence as to whether this is required, nor how it would be enforced if it were required. Practically speaking, there are four ICANN approved DRPs, none of which are related, and thus it seems impractical and unlikely for one DRP to follow a decision of another DRP. Some authors note that there are differences in the types of decisions arrived at by the DRPs and that these differences in attitudes, as well as the differences in composition of the DRPs, create a phenomenon known as "forum shopping."⁹⁰ Contrasted with this dilemma is the ACPA, which is bound by precedent and is therefore more likely to make consistent decisions.

It must be noted that the UDRP is not set up to deal with complex legal issues. The UDRP only deals with domain name disputes between a trademark or service mark holder and the domain name holder (alleged cybersquatter). If a complainant has several legal issues to resolve, such as allegations of false advertising or unfair competition, he is better off to refer these issues to the federal court system.⁹¹ Additionally, the federal court system is better suited to hear matters involving nuances or emerging issues in trademark law, as well as cases that have significant issues relating to the finding of facts and credibility.⁹² The ACPA, as a civil action, also allows for discovery during which time a plaintiff may have an opportunity to gather evidence relating to proof of bad faith.⁹³

There is no clear choice as to which method of resolution should be applied to domain name disputes. The UDRP offers a cheap and expedient method for trademark holders to regain control of domain names from cybersquatters. The ACPA allows for more remedies, but at a significant cost in both time and legal fees. The UDRP breaks down the barriers of jurisdiction, but contains little certainty regarding the outcome of certain issues, especially in complex legal areas. The ACPA engages the US federal court system, which is fully equipped to deal with a multitude of legal issues, but is dependent on US jurisdiction. What this analysis boils down to is that, depending on the needs of the client, there are alterna-

⁹⁰ See Mueller, *supra* note 12 for a full discussion on this topic.

⁹¹ S. Edelman, "Cybersquatting Claims Take Centre Stage" (2000) vol. 18, no.1 Computer & Internet Lawyer 1 at 4.

⁹² *Ibid.*

⁹³ *Ibid.*

tives from which to choose. In *Broadbridge Media L.L.C. v. Hypercd.com*, the Court determined that an action under the ACPA could be initiated at any time before, during, or after the initiation of proceedings under the UDRP.⁹⁴ Thus it may be most prudent to initiate both proceedings, ensuring a speedy transfer of the domain name under the UDRP, while resolving the broader legal issues and leaving open the possibility of damages under the ACPA.

V. CONCLUSIONS

AS WE HAVE SEEN, since the fall of 1999 there have been two regimes created to deal with the problem of cybersquatting on the internet. The first is an ADR regime, engaged by utilizing ICANN's UDRP. The second regime is under US federal trademark law and the ACPA. Taking into account the strengths and weaknesses of the two systems, it is concluded that the choice of forum depends on the needs of the client, noting that it is entirely possible to engage both regimes simultaneously to arrive at the best possible outcome.

Will these two alternatives wipe out cybersquatting as a problem facing e-commerce? Probably not, as cybersquatters have shown an ability to alter their behavior in order to stay one step ahead of the law. The legal development in this field (as in most areas of the law) is reactionary.

Will the introduction of new gTLDs eradicate the problem of cybersquatters? Again, the answer seems to be probably not. As it currently stands, ICANN has only approved seven new gTLDs. The practice for businesses has been to register their distinctive name across several gTLDs in order to ensure that internet users find their way to their site. Thus, even with new gTLDs, there will always be the enterprising cybersquatter who is one step ahead of businesses in registering domain names.

The only way to get tougher on cybersquatters is to further regulate the registration of domain names, requiring registrars to check for potential trademark infringements before they arise, and requiring those who register domain names to provide further documentary evidence of their claim to a domain name before they are allowed to register the domain name. In effect, this would remedy the problem at its source.

This approach has been attempted to a certain degree, amidst much controversy, by the registrars administering the new gTLDs. We will soon see how effective this approach is at protecting the rights of trademark holders. In the meantime, disputes in the <.com>, <.net>, and <.org> TLDs must rely on the UDRP and the ACPA to settle their disputes.

⁹⁴ 106 F. Supp. 2d 505 at 509 (2000).