CENTRAL EUROPEAN UNIVERSITY

The Relationship between Domain Names and Trademark Law

by Adam Dunn

LL.M. SHORT THESIS
COURSE: Intellectual Property Law
PROFESSOR: Caterina Sganga
Central European University
1051 Budapest, Nador utca 9.
Hungary

Table of content

Abstract

The purpose of this paper is to conduct of survey of the law concerning domain name disputes (specifically in the context of cybersquatting) and their legal position under trademark law in cyberspace. Further, I will examine possible solutions going forward.

In Chapter One, I will provide an overview of domain names and some issues associated with domain names in the context of the Internet.

In Chapter Two, I will provide an overview of trademark law, its history and modern practice as it pertains to US, UK, Germany and international law.

In Chapter Three, I will provide an overview of cybersquatting, detailing its history, while also surveying its status today in the US, UK, and Germany.

In Chapter Four, I will discuss avenues for remedies available in relation to cybersquatting through ICANN, WIPO and the national courts of the US, UK and Germany.

In Chapter Five, I will discuss first some jurisdictional issues related to combatting cybersquatting, and then proceed with a survey of proposed solutions to cybercrime while also pointing out potential benefits and drawbacks to each solution.

Introduction

The Internet is a global network of interconnected networks operating by way of the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol systems.[1] The Internet was not formed initially for the commercial purposes that we have come to expect from it today. Rather, the Internet was birthed for the initial purpose of achieving an efficient method of communication between a network of computers as a result of research conducted, and funded, by the U.S. Government through the United States Advanced Research Project Agency (ARPA).[2] This experimental network, linking just four computers initially in 1969, came to be known as ARPANET.[3] Throughout the 1970's and 1980's, the internet was primarily academic and governmental in nature. During these formative years of the Internet, a way was needed to direct communication/information to the proper point from one computer to another. Through a process of trial and error, the current Domain Name System came about. In this system, there are two addresses. One address is a computer–readable Internet Protocol (IP) address, which is extremely difficult for humans to remember in order to send information due to it being a rather cryptic looking set of numbers.[4] The other address is a human-readable name.[5] This human-readable name is what we now call a 'domain name'. So long as the system was purely academic or governmental, there was no issue in regard to potential infringement of intellectual property trademark rights in relation to domain names.

[1] David Lindsay, International Domain Name Law 1, (Hart Pub Ltd. 2007).
[2] Id. at 1.
[3] Id. at 1
[4] Id. at 6.
[5] Id. at 6.

However, the 1990's brought about the privatization of the Internet backbone, and thus, commercialization of the Internet.[6] It is precisely this commercialization which set up the current dynamic between domain names and trademark law. Trademark law initially developed in order to give holders of trademarks intellectual property rights. In contrast, the domain name system was not developed with the purpose of awarding some kind of intellectual property right to the holder of a domain name. The fact that a domain name registrant did not have to be the trademark owner led to considerable instances of what came to be called 'cybersquatting'. Cybersquatting is a where a domain name is registered, sold or used with the intent of profiting from the goodwill from someone else's trademark.[7] Cybersquatting can result in very real damage to the trademark by diminishing the distinctiveness of the mark or using it in a way detrimental to the holder of mark.

The increasing number of cybersquatting cases resulted in a proliferation of cases coming through court systems world-wide, thus necessitating the need for new laws to deal with the emerging cyberspace threat. The United States, for its part, introduced the federal Anti-cybersquatting Consumer Protection Act (ACPA), making cybersquatting a crime, to deal with the new class of claims.[8] ACPA defines cybersquatting as: 'the registration or use of a trademark as a domain name in bad faith with an intention to profit from the mark'. The United Kingdom has not instituted a specific statute in relation to cybersquatting, but deals with it in a common law approach through the Courts, which typically apply trademark law in such notable cases as 'Harrods', 'One-in-a-Million' and 'The French Connection'.[9] Likewise in Germany, there is no

[6] Lindsay, David. International domain name law at p.11. Oxford: Hart Pub., 2007. Print.
[7] Christopher Varas, *Sealing the Cracks: A Proposal to Update the Anti-cybersquatting Regime to Combat Advertising-based Cybersquatting*, 3 J. of Intell. Prop. L. 246, 246-261 (2008).
[8] See Lindsay, *supra* at 96.
[9] Ian Tollet, *Domain Names and Dispute Resolution*, 23 (2) World Pat. Info. 169, 169-175 (2001).

specific statute addressing the crime of cybersquatting. Although Germany is a civil law jurisdiction, cybersquatting and domain name disputes are typically resolved through the court system in conjunction with 12 BGB (German Civil Code).[10]

Due to the overwhelming demand and stress on national court systems, Internet Corporation for Assigned Names and Numbers (ICANN) promulgated a private arbitral forum for the resolution of domain name disputes called Uniform Dispute Resolution Process (UDRP)[11] The UDRP is an international arbitration forum that is generally preferred by disputants because the decisions are delivered relatively quickly and it is typically more inexpensive than litigating in a national court or in multiple national courts, depending on the nature of the dispute.

However, the UDRP has its detractors. The issues cited by the detractors are that there is no doctrine of stare decisis (obligatory following of case precedent), which leads to inconsistency in judgments.[12] Furthermore, the UDRP offers limited remedies to dispute participants. The only remedies available are: cancellation of offending domain name or transfer of domain name.[13] Consequently, the world and academia have been searching for a better system to address domain name/cybersquatting issues.

[10]Lambert Pechan, *Domain Grabbing in Germany: Limitations of Trade Mark Protection and How to Overcome Them*, 7 (3) J. of Intell. Prop. L. &Prac. 166 (2012).
[11]Lisa M. Sharrock, *The Future of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions from Within the UDRP Framework*, 51 Duke L. J. 817 (2001).
[12]*Id.* at 818.
[13] Paragraph 4(i) of the UDRP Rules

Chapter One: Domain Names

In this chapter, I will be discussing how domain names came about and why they are the key markers on the internet for direction information and typed searches to the proper location. I will work through the history of the domain names, how the domains are constituted, the addressing function of a domain name, the elements necessary for an infringement claim, and the general domain name infringement defenses. It is important to note that unlike trademarks, there are no international treaties regulating domain names.

1.1. Domain Name History

As previously stated in this paper, the early years of the Internet were filled with growing pains and the search for ways to more efficiently streamline the information being sent back and forth between networks. In the infancy of the development of ARPANET, each host computer was required to keep a copy of the <hosts.txt> file, thus requiring that when a new host was connected to ARPANET, the <host.txt> file needed to be updated, and copies of the new file be sent to all connected hosts.[14] The <hosts.txt> file is a simple text file that was maintained by the Stanford Research Institute – Network Information Center (SRI-NIC).[15] It was developed to provide a map between names of computers (hosts) and the IP network addresses where they could be reached.[16] Due to the growth of the Internet, the costs for maintaining the <hosts.txt.> file became too much and furthermore was not an efficient means of controlling information

[14]See Lindsay, *supra* at 4.
[15]P. V. Mockapetris& K. J. Dunlap, *Development of the Domain Name System,* 18 ACM Computer Comm. Rev. 123 (1988).
[16] K. Harrenstein, M. Stahl and E. Feinler "Dod internet host table specification" RFC 952, 123 October(1985).

going to a host.[17] In order for the Internet to continue its expansion, a more streamlined distributed naming system needed to be developed.

There were several naming systems bandied about in the search for a suitable distributed naming system, such as DARPA Internet's IEN116, XEROX Grapevine (Birrell 8) and Clearinghouse systems (Oppen 83).[18] Each of these systems had plausible benefits, however each also had shortcomings in relation to the purpose of streamlining communications between hosts.[19] Thus, the Domain Name System, with its flexibility, was developed to deal with the initial issues related to the ARPANET name and addressing system.

1.1.1 Importance of DNS and Mapping Addresses to Domain Names

A computer is a machine that allows for the processing of information in binary form.[20] Similar to the mechanism for sending a physical letter to a physical address, in order to successfully send information across a network from a source to a destination, each address must be unique. Internet addressing issues are dealt with through the IP protocol.[21] In the case of networks sending and receiving information to the proper address, there are actually two addresses to consider.

One address is a computer-readable IP address. This form of the address was originally incepted through IP4 address, which were structured under a rigid classes based on number of

[17] K. Harrenstein, M. Stahl and E. Feinler "Dod internet host table specification" RFC 952, October, 1985 (at p. 123)
[18] K. Harrenstein, M. Stahl and E. Feinler "Dod internet host table specification" RFC 952, October, 1985 at p. 123
[19] K. Harrentstein, M. Stahl and E. Feinler Id. at 123 – 124. 'The IEN116 services seemed excessively limited and host specific, and IEN116 did not provide much benefit to justify the costs of renovation. The XEROX system was then, and may still be, the most sophisticated name service in existence, but it was not clear that its heavy use of replication, light use of caching, and fixed number of hierarchy levels were appropriate for the heterogeneous and often chaotic style of the DARPA Internet.'
[20] See Lindsay, *supra* at 4.
[21] See Lindsay, *supra* at 4.

bits allocated to the network prefix.[22] However, the rapid of expansion of the Internet in the 1990's necessitated the development of a new address space, IP6. IP6 addresses consist of eight 16-bit integers separated by colons.[23] The IP4 and now IP6 address are a very complicated string of numbers that would be mostly incomprehensible to the average web surfer. A typical string would look like this:

192.0.43.10 (IPv 4); or

2001:500:88:200:0:0:0:10 (IPv6)[24]

A second address is assigned to each host computer connected to the Internet. This address is a human-readable name, known now as a domain name.[25] 'The main purpose of the DNS is to map domain names to IP addresses.' This method of mapping unique domain names to unique IP addresses was the right system to support the development of hyperlinking mechanisms (in the form of Uniform Resource Locators) that created the World Wide Web, and thus the widespread commercialization of the internet.[26] Currently, Internet Corporation for Assigned Names and Numbers 'ICANN' manages DNS and designs policies for its operations.(change this sentence around.. its copy and pasted)

This development is significant to the average user of the Internet today and in the context of holders of trademark rights. Without the domain name, there would generally be no intellectual property issues concerning the address because there would be no potential for degradation of a mark or goodwill of an entity holding a trademark resulting from confusion as to whether the domain name holder is the proprietor of the trademark. Thus, the fateful day in

[22]See Lindsay, *supra* at 5.
[23]See Lindsay, *supra* at 6.

[24]M. Tariq Banday, *Recent Developments in the Domain Name System,* 31 Int'l J. of Computer Applications, Found. of Computer Sci. 18 (2011).
[25]See Lindsay, *supra* at 6.
[26]Steven Wright, *Cybersquatting at the Intersection of Internet Domain Names and Trademark Law,*14 (1) IEEE Comm. Surveys & Tutorials 194 (2012).

1971 when Peggy Karp first suggested the concept of assigning human readable names to addresses[27] continues to reverberate through the IP Law and world courts up to today.

1.2 – Domain Name Space and Top Level Domains

1.2.1 Domain Name Space

David Lindsay notes in his book 'The Domain Name Space (DNS) is organised hierarchically around a root and tree structure'.[28] This structure provides the establishing the basis for the DNS tree hierarchy.[29] The DNS tree has a maximum limit of 127 levels, customarily divided into the hierarchical levels from Top-Level Domains (TLDs), Second-Level Domains (2LDs), Third-Level Domains (3LDs) all the way to Nth-Level Domain (which means the host computer name).[30]

Tariq Banday further describes the structure in his article: 'The topmost level in the hierarchy is the root domain, which is represented as a dot (".").[31] The next level in the hierarchy is called the top-level domain (TLD). TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "info" in "www.banday.info".[32] By implementing this structure, it allows the administrators of the 'root zone' or 'root domain' to control what TLDs are recognized by DNS.[33]

The impetus behind implementing the DNS was to decentralize the administration of Internet naming and address functions. Due to the hierarchical nature of DNS, the responsibility

[27]See Lindsay, *supra* at 4.
[28]See Lindsay, *supra* at 8.
[29] See Lindsay, *supra* at 8.
[30]See Lindsay, *supra* at 8.
[31]See Banday, *supra* at 18.
[32]*Id.* at 18. (Banday)
[33]*Id.* at 18. (Banday)

for managing and assigning names at different levels could be given to a larger selection of entities.[34]

This decentralization was a key development in the growth of the Internet as it took the overwhelming responsibility for assigning and managing names from one entity and spread it out to multiple entities. This is significant because one entity can only monitor so much information. Multiple entities assigning and managing names allowed the Internet the space to grow.

1.2.2 Top-Level Domains (TLDs)

i. Top-Level Domains: Top-level Domains are included in all domain names.[35] There are generally two kinds of TLDs: generic TLDs (gTLDs) and country code TLDs (ccTLDs).[36]

ii. Generic TLDs: Regarding generic TLDs, RFC 1591 released in March 1994 listed only seven initial TLDs and the uses envisaged for them.[37] The seven are as follows:

.com – intended for commercial entities

.edu – intended for US educational institutions that are 4 year colleges or universities

.gov – limited currently to US federal government agencies

.in – limited to organizations established by international treaties

.mil – limited to US military

.net – intended only for organizations providing network infrastructure. However, the restriction was removed in 1996.

.org – intended as miscellaneous TLD for organization that didn't fit elsewhere. The restriction was also removed in 1996[38].

[34] *Id.* at 18. (Banday)

[35] See Lindsay, *supra* at 9.

[36] Catherine R. Easton, *ICANN's Core Principles and the Expansion of Generic Top-level Domain Names*, 20 (4) Int'l J. of L. & Info. Tech. 275 (2012).

[37] See Lindsay, *supra* at 9.

Due to the rapid expansion of the Internet, the number of gTLDs now numbers at least thirty. Some registrations of gTLDs are open and some have restrictions. For example, .com, .net. and .org were open for registration without restrictions.[39]

iii. New Generic TLDs: In examining generic TLDs, one can further split them into two separate categories: sponsored (sTLDs) and non-sponsored (uTLDs).[40]

iv. Sponsored TLD (sTLD): An example of a sponsored string would be the following: .asia, .cat, .jobs, and .travel. These sponsored strings can have differing eligibility criteria. Some are open registration, however some have restrictions, such as the .cat string, which is for the Catalan linguistic and cultural community.[41]

v. Country Code TLDs (ccTLDs): ccTLDs are TLDs based on geographical or national boundaries and consists of two letter abbreviations standing for the countries.[42]

There has been a considerable amount of controversy worldwide related to Top-Level Domains. One might wonder why this seemingly mundane area of classifying a domain would engender so much controversy. The reason is best summed up by analogy of Dr. Milton Mueller: 'TLDs may appear to be an obscure topic, and an unlikely basis for a global controversy. Yet the system for distributing the right to create and manage a TLD is fundamental to the operation of the Internet. Just as the scarcity of radio frequencies provided the problem around which systems of mass media regulation crystallized in the 1920s, so domain naming will be the catalyst of a new system of Internet governance'.[43]

[38]See Lindsay, *supra* at 9.
[39]See Easton, *supra* at 275.
[40]See Easton, *supra* at 275.
[41]See Lindsay, *supra* at 9.
[42]Milton Mueller, *The Battle Over Internet Domain Names: Global or National TLDs?*, 22 (2) Telecomm. Pol'y 90 (1998).
[43]See Mueller, *supra* at 89.

Though Dr. Mueller wrote his article in 1998, Dr. Mueller's point is still valid today and the implications are huge, as those who control the TLDs will control the internet. As he also notes in his article, this seemingly trivial matter has already taken up the attention of many US federal agencies, the European Union ("EU") and many service providers.[44] The fight over control and access to TLDs will most likely continue to the foreseeable future.

1.3 – ICANN and Domain Name Infringement Claims

1.3.1 ICANN

ICANN is a nonprofit organization based out of California which regulates the allocation of domain names and thus occupies a position of great power in relation to the Internet governance.[45] However, as noted by David Lindsay, 'the term 'governance' in relation to the internet is widely acknowledged to be imprecise, with no single accepted definition'. Lindsay continues, adding: 'there are many uses of governance: for example, it refers to the minimal state; corporate governance; and new public management...'.[46]

ICANN obtained this ability to allocate domain names through a contract in 1999 with the US Department of Commerce, ICANN and Network Solutions Inc., although the legal authority to enter these agreements regarding governance is uncertain.[47] ICANN's position as the allocator of domain names meant that when domain name registrants began registering registered trademarks as domain names, it was under heavy pressure to design a solution to the increasing amount of intellectual property infringement.

[44]See Mueller, *supra* at 89. 'The problem has already engaged more than a dozen US federal agencies acting through an interagency committee, the International Telecommunication Union, the European Union, many Internet users and service providers, and the Internet Society".
[45]See Easton, *supra* at 276.
[46]See Lindsay, *supra* at 27.
[47]See Lindsay, *supra* at 48. ("Authority over the DNS is therefore defined mainly y means of the agreements between the parties rather than by reference to any independent, external source of legal authority, such as an international treaty'.)

This pressure prompted ICANN to request a recommendation from the World Intellectual Property Organization ("WIPO") regarding a plan of action to address the issue.[48] In 1999, ICANN established the Uniform Dispute Resolution Policy based in part on the recommendation of WIPO. The UDRP and its elements and defenses will be discussed more fully in chapter four.

[48]See Lindsay, *supra* at 103.

Chapter Two: Trademarks

Introduction: In this section, I will describe what a trademark is, the history and development through time, and a comparison of US Law, UK Law, and German Law.

2.1 – Trademark and History of Trademark

2.1.1 What is a Trademark?

Although, different jurisdictions utilize various definitions of trademark, a trademark is generally understood to be "a symbol, word, or words legally registered or established by use as representing a company or product".[49] It is what distinguishes your product from the next product. In the modern ultra-competitive world, companies and businesses spend millions to make their product stand out from the pack, and thus we begin to ascertain why trademarks are so fiercely protected today.

The Office for Harmonization in the Internal Market ("OHIM") goes so far as to state on its official site that 'your trademark may be your most valuable asset... and is crucial to the success of your business'.[50] The trademark doesn't simply identify a good, but also identifies the source of the good[51] as well as sometimes implying quality or lifestyle.[52] It is also useful to note that trademarks are not limited to printable characters, but can also be colors or scents.[53]

Thus, there are two general purposes for having trademark protection in place:

1) to protect the owner of a mark's investment; and

[49] Oxforddictionaries.com. 2014. trademark: definition of trademark in Oxford dictionary (British & World English). [online] Available at: http://www.oxforddictionaries.com/definition/english/trademark [Accessed: 25 Feb 2014].
[50] Oami.europa.eu. 2014. Trade marks basics - CTM. [online] Available at:https://oami.europa.eu/ohimportal/en/trade-marks-basics [Accessed: 25 Feb 2014].
[51]Shoen Ono, Overview of Japanese Trademark Law 1 ch.2 (2nd ed. Yuhikaku 1999).
[52]Graham Dutfield& Uma Suthersanen, Global Intellectual Property Law 139 (Edward Elgar Publ'g 2008).
[53]See Wright, *supra* at 195.

2) for the benefit of the consumer (so that they may identify proper good of maker)[54]

2.1.2 Evaluating Trademarks

Steven Wright notes that "Trademarks are generally evaluated based on the following scale of distinctiveness:

- Fanciful - coined terms with no common place or dictionary meaning.
- Arbitrary - dictionary words in common usage that do not describe the item they are attached to
- Suggestive - words that require some imaginative leap to establish a connection to the item they are attached to
- Descriptive - words that specifically describe some characteristics of the item they are attached to
- Generic - words in common usage as the name of item.

It is important to note what these distinctions mean. Fanciful, Arbitrary or Suggestive words are deemed "inherently distinctive and recognized as trademarks upon usage in commerce".[55] Words that are generic can never be trademarks. However, descriptive words may be able to qualify for trademark protection if 'it can be shown that secondary meaning for those words as a trademark has been established in the market".[56]

It will be important to keep these items in mind when contrasting the differences between trademark law. For example, to qualify for a trademark protection, one would need to show that it is distinct and it is in use in commerce.[57] Furthermore, this protection would generally only extend to the jurisdiction which grants it, not the entire world. However, as previously discussed

[54]Leslie Suzanne Park,*ThePrimary Trademark Identifier Requirement: A Change to Current Trademark Law*, 2013 Seton Hall L. ERepository1 (2013).
[55]See Wright, *supra* at 195.
[56]See Wright, *supra* at 195.
[57] Law.cornell.edu. 2014. Trademark | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute. [online] Available at: http://www.law.cornell.edu/wex/trademark [Accessed: 26 Feb 2014].

in the domain name section, there is no requirements for registering a domain name particularly. One need just register with a registered provider and the domain name is valid the whole world over. Thus, in examining what a trademark is, it is important to keep in mind the distinctions between it and domain names.

Before proceeding to an examination of US, UK and German trademark law, it would first be beneficial to provide a brief background on trademark history.

2.1.3 History of the Trademark

Trademark law has developed over the course of many years. In fact, the concept of trademarks, even if not trademarks in the modern sense, have been around for thousands of years. There is evidence of 3,000 year old pottery imprinted with the mark of the proud potter.[58] Likewise, there is evidence ranging from the ancient Greek and Roman societies imbuing their products with marks, to guilds in the Middle Ages using marks to identify their products.[59] All of this illustrates that the concept trademarks are interwoven into the fabric of our commercial human civilization.

Unfortunately for the potter and all others imprinting their business mark on products, there was no in general no tacit judicial recognition of trademarks until Sandforth's Case in 1584.[60] From this first case, there has been a gradual evolvement of trademark law, from the nineteenth century common law tort of 'passing off', to full-fledged modern statutes dealing specifically with trademark. It is clear that there has been an increase in, and recognition for the need of, trademark protection due to a trademark's importance in goodwill and value as a means of identifying the business and protecting consumer deceit about goods. This was explicitly

[58]See Ono, *supra*ch 2 at 1.
[59] See Ono, *supra*ch 2 at 2.
[60]Sheldon W. Halpern, Craig Allen Nard & Kenneth L. Port, Fundamentals of United States Intellectual Property Law 290 (Kluwer Law Int'l 2011).

recognized through a series of ever increasing protection, from the Paris Convention to the modern TRIPs Agreement.

2.1.4 The Paris Convention

The Paris Convention was came into effect in 1884 and was one of the first treaties concerning the protection of intellectual property, and in particular, trademarks. As of 2014, the Convention is still in effect. It is interesting to note that the Paris Convention did not attempt to define trademark. This is interesting because the drafters of the Convention intentionally did this in order to be consistent with one of the fundamental principles of international trademark protection, the principle of territoriality.[61]

The Max Planck Institute for Intellectual Property describes the principle thusly:

> "According to the principle of territoriality, the scope of protection of an IP right is limited to the territory of the State where the right is granted. Thus different, and from each other independent, national and regional protection rights which are subject to different legal regimes may exist alongside each other on the same immaterial good. The principle of territoriality forms the basis for both national and regional IP laws as well as multilateral conventions on intellectual property protection and can therefore be considered an internationally recognised principle structuring the protection of IP rights".[62]

The principle is important enough that it was included in the Paris Convention[63] under Article 6(3), which states:

"A mark duly registered in a country of the Union shall be regarded as independent of marks registered in the other countries of the Union, including the country of origin".[64]

[61]See Lindsay, *supra* at 172.
[62] Ip.mpg.de. 2014. Max Planck Institute for Innovation and Competition- The Concept of Territoriality and its Impact on Intellectual Property. [online] Available at: http://www.ip.mpg.de/en/pub/research_teaching/ip/main_areas/concept_of_territoriality.cfm [Accessed: 25 Feb 2014]
[63]James E. Darnton, *Coming of Age of the Global Trademark: The Effect of Trips on the Well-Known Marks Exception to the Principle of Territoriality,* 20 (1) The Mich. St. C. of L. Int'l L. Rev. 16 (2011).

Thus, the Paris Convention was a groundbreaking treaty in that it memorialized in writing many important principles, perhaps the most important being the principle of territoriality, which is still utilized in international trademark law today. Furthermore, it provided the basic foundation and structure for more modern treaties such as TRIPs.

2.1.5 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs)

The Uruguay Round of negotiations birthed the TRIPs agreement. Further negotiations were needed after the Paris Convention and subsequent other conventions because none of them provided particularly strong enforcement mechanisms and many signatories frequently diddled on their obligations in regard to the conventions.[65] Thus, the TRIPs Agreement was a means of establishing an enforcement mechanism for the Paris Convention amongst member countries.[66] Moreover, TRIPs is important because it requires compliance with Articles 1-12 and 19 of the Paris Convention.[67]

The Paris Convention and TRIPs agreement are both important in that they give the modern era of trademark law necessary guidelines. The Paris Convention in particular provided the framework for modern trademark law. I will now conduct a survey of law ranging from international trademark law to national trademark law in the US, UK and Germany.

[64] Wipo.int. 2014. WIPO-Administered Treaties: Paris Convention for the Protection of Industrial Property. [online] Available at: http://www.wipo.int/treaties/en/text.jsp?file_id=288514#P174_27991 [Accessed: 26 Feb 2014]. Article 6(3)
[65]Duncan Matthews, Globalising Intellectual Property Rights 8 (Routledge 2003).
[66]See Lindsay, *supra* at 172.
[67]See Lindsay, *supra* at 172.

2.2 International Trademark Law

2.2.1 World Intellectual Property Organization (WIPO)

The United Nations (UN) established WIPO in 1967 in an effort to enforce the measure of the Paris Convention and furthermore, to harmonize the intellectual property laws of varying national states.[68] According to the WIPO mission statement, their mission is to "lead the development of a balanced and effective international intellectual property (IP) system that enables innovation and creativity for the benefit of all".[69] One need only look at all the services WIPO provides (a lot), and how many members they have (186 countries), to get a look at how influential this organization is. Below is a sample of services they provide:

• a policy forum to shape balanced international IP rules for a changing world;

• global services to protect IP across borders and to resolve disputes;

• technical infrastructure to connect IP systems and share knowledge;

• cooperation and capacity-building programs to enable all countries to use IP for economic, social and cultural development;

• a world reference source for IP information[70]

A further look illustrates the extent of their influence over modern intellectual property law. WIPO was involved in the initial International Ad Hoc Committee formed for the purpose of determining governance on the Internet, which eventually brought about ICANN.[71] ICANN then solicited WIPO to provide a recommendation on a model for dispute resolution of domain

[68]See Matthews, *supra* at 8.
[69] Wipo.int. 2014. Inside WIPO. [online] Available at: http://www.wipo.int/about-wipo/en/index.html [Accessed: 26 Feb 2014].
[70] Wipo.int. 2014. Inside WIPO. [online] Available at: http://www.wipo.int/about-wipo/en/index.html [Accessed: 26 Feb 2014].
[71]See Lindsay, *supra* at 38.

names, resulting in the UDRP.[72] Furthermore, ICANN has designated them a forum for dispute resolution.[73] The above illustrates the huge impact WIPO has on intellectual property and trademark law.

2.2.2 European Union via Office for Harmonization in the Internal Market (OHIM)

OHIM is an agency of the European Union and was formed in 1994 specifically for the purpose of registration and protection of trademarks and designs.[74] OHIM is engaged with international community to foster greater protection for trademarks across the European Union.[75]

2.2.3 World Trade Organization (WTO)

WTO is a global international organization created in 1994 out of the Uruguay Round negotiations with 159 current members that gives the following as its functions:

• Administering WTO trade agreements

• Forum for trade negotiations

• Handling trade disputes

• Monitoring national trade policies

• Technical assistance and training for developing countries

• Cooperation with other international organizations[76]

[72]See Lindsay, *supra* at 106.
[73]See Lindsay, *supra* at 116.
[74] Oami.europa.eu. 2014. Who we are. [online] Available at: https://oami.europa.eu/ohimportal/en/who-we-are [Accessed: 26 Feb 2014].
[75] Oami.europa.eu. 2014. Who we are. [online] Available at: https://oami.europa.eu/ohimportal/en/who-we-are [Accessed: 26 Feb 2014].
[76] Wto.org. 2014. WTO | About the organization. [online] Available at: http://www.wto.org/english/thewto_e/thewto_e.htm [Accessed: 26 Feb 2014].

The WTO is important because it was instrumental in bringing about the TRIPS Agreement, which is the modern treaty which provides the framework for intellectual property law.

2.3 United States Trademark Law

The United States Trademark law is divided under a dual system of state[77] and federal[78] protection. A trademark can be registered or unregistered, but a registered trademark offers greater protection for its holder.[79] For the purposes of this paper, I will deal predominately with federal U.S. trademark law as opposed to state law. There was long recognized a need for trademark protection in the U.S., as evidenced by the enactment in 1870 of the first federal trademark law.[80] However, that law was held unconstitutional and thus would be another 76 years until a comprehensive, constitutional federal trademark law could be enacted.[81]

The United States enacted the Lanham Act in 1946 to specifically deal with trademark law.[82] The Lanham Act defines a trademark thusly:

"A trademark is any word, name, symbol, or design, or any combination thereof, used in commerce to identify and distinguish the goods of one manufacturer or seller from those of another and to indicate the source of the goods".[83]

a) Elements for a Trademark Infringement Action for Direct Infringement

To prove trademark infringement under the federal Lanham Act, you must prove:

1) a protectable interest in a valid trademark

[77] Robert C. Lind, Trademark Law 5 (N. Carolina Academic Pr 2006).
[78] See Lind, *supra* at 68.
[79] Law.cornell.edu. 2014. Trademark | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute. [online] Available at: http://www.law.cornell.edu/wex/trademark [Accessed: 27 Feb 2014].
[80] See Lindsay, *supra* at 173.
[81] See Lindsay, *supra* at 173.
[82] Mary LaFrance, Understanding Trademark Law 6 (LexisNexis 2009).
[83] Lanham Act, § 45, 15 USC § 1127.

2) the defendant's use of that mark in commerce; and

3) the likelihood of consumer confusion.[84]

Here, we can see that there is a three step analysis in ascertaining whether a trademark infringement has occurred. Furthermore, federal courts have adopted a multi-factor balancing test, although it is important to note that no single factor is determinative and that the list of factors is non-exhaustive.[85] Some of the factors considered by courts are:

• similarity of marks

• competitive proximity

• strength of plaintiff's mark

• consumer sophistication

• actual confusion; and

• defendant's good faith (or lack thereof)[86]

For the purposes of this paper, it is important to note that courts initially had trouble with domain names and whether use of them was a trademark infringement issue.[87] Part of the reason for this is because a domain name is really an address, and trademark law was not developed to give protection and remedies to addresses. However, as referenced previously in this paper, modern consumers equate the domain name address with the business owner mark generally. For instance, a consumer would generally assume that goldenarch.com is registered to McDonalds. The Anti-Cybersquatting Protection Act (ACPA) largely alleviated this tension of courts struggling to fit domain name infringement cases into traditional trademark law cases. I will discuss ACPA and its effects on domain name cases and trademark law in chapter three on

[84]See Lind, *supra* at 68.
[85]See Lafrance, *supra* at 140.
[86]See Lafrance, *supra* at 140 - 157.
[87]See Lafrance, *supra* at 183.

cybersquatting.

b) Defenses to a Trademark Infringement Action

Similar to domain name infringement, there are also defenses that one can assert to negate these elements of a trademark infringement claim. The following are a few of the defenses available:

• valid license

• statute of limitation

• laches

• unclean hands

• fair use

• First Amendment

• first sale doctrine[88]

There a few other defenses available, but for the interest of this paper and relevance, I only list the above. For a complete reading of defenses, please see Robert Lind's "Trademark Law".

2.4 United Kingdom Trademark Law

Similar to the United States, for many years there were demands for legal protection of marks in the United Kingdom ("UK"). The courts of equity were sought initially as most plaintiffs wanted an injunction, i.e.; they wanted the infringer to stop passing off or diluting the mark goodwill.[89] However, a more streamlined approach was needed and commercial interests pushed for a system of registering marks. Thus, in 1875, the United Kingdom introduced the

[88]See Lind, *supra* at 149.
[89]W. William Rodolph Cornish & David Llewelyn, Intellectual Property 607 (Sweet & Maxwell 2007).

Trade Marks Registration Act.[90] This act became the precursor to the modern acts such as the Trade Mark Act of 1934 and Trade Mark Act of 1994. It is of note that the UK is part of the EU and that the 1994 Act expanded the scope of its trade mark law to fall in line with an EC Directive.[91]

The 1994 Trade Mark Act ("TMA") defines 'trade mark' to mean:

"Any sign capable of being represented graphically which is capable of distinguishing good or services of one undertaking from those of other undertakings.

A trade mark may, in particular, consist of words (including personal names), designs, letters, numerals or the shape of goods or their packaging".[92]

It should be noted that unlike in the US, the UK does not explicitly provide protection for unregistered trademarks under the Trade Mark Act.[93] However, if a mark has been used in the course of business but is unregistered, it's possible to prevent use by a third party by bringing an claim under the common law action of 'passing off', though it should be noted that succeeding in this action is tougher than a trademark infringement action.[94] The Intellectual Property Office ("IPO") notes further that whether an unregistered mark will be protected is contingent on the circumstances such as:

• "Whether, and to what extent, the owner of the unregistered trade mark was trading under the name at the date of commencement of the use of the later mark;

[90]See Cornishand Llewelyn, *supra* at 608.
[91]See Ono, *supra*ch 2 at 3.
[92] Trade Marks Act 1994 (UK) s 1(1)
[93]Lorna Brazell, Intellectual Property Law Handbook 55 (1st ed. The Law Soc'y 2008).
[94]See Brazell, *supra* at 55. ("in passing off it is necessary to prove that the trade mark has acquired goodwill and that the proprietor has suffered damage. Neither of which is necessary to establish a trade mark infringement under TMA")

• "Whether the two marks are sufficiently similar, having regard to their fields of trade, so as to be likely to confuse and deceive (whether or not intentionally) a substantial number of persons into thinking that the junior user's goods and services are those of the senior user";

• "The extent of the damage that such confusion would cause to the goodwill in the senior user's business".[95]

Now that it is established what qualifies for protection under the Trade Mark Act, let us examine the elements necessary for a trade mark infringement action.

a) Elements for a Trade Mark Infringement Action

The Trade Mark Act of 1994 provides the following instances of infringement:

• A person infringes a registered trade mark if he uses in the course of trade:

a sign which is identical with the trade mark in relation to goods or services which are identical with those for which it is registered.[96]

• A person infringes a registered trade mark if he or she uses in the course of trade a sign where because:

a) the sign is identical with the trade mark and is used in relation to goods or services similar to those for which the trade mark is registered; or

b) the sign is similar to the trade mark and is used in relation to goods and services identical with or similar to those for which the trade mark is registered,

c) there exists a likelihood of confusion on the part of the public, which includes the likelihood of association with the trade mark.[97]

[95] Ipo.gov.uk. 2014. Intellectual Property Office - Infringement, What is trade mark infringement?. [online] Available at: http://www.ipo.gov.uk/types/tm/t-other/t-infringe.htm [Accessed: 27 Feb 2014].
[96] Trade Marks Act 1994, s. 10(1)
[97] Trade Marks Act of 1994, s. 10(2)

The crucial part of the wording above in both instances of infringement is that it is 'use in the course of trade'.[98] The TMA provides a non-exhaustive list of instances of use in the course of trade such as:

- affixing the sign to goods or its packaging
- offering or exposing goods for sale, putting them on the market, or stocking them for those purposes under the sign, or offering or supplying services under the sign;
- importing or exporting goods under the sign;
- using the sign on business paper or in advertising[99]

Similar to the US Courts, the English Courts initially struggled to fit the concept of domain name infringement into traditional trade mark law concepts. For example, does simply registering a domain name that is a registered trade mark of another constitute 'use in the course of trade'? I will attempt to answer this question in the next chapter on cybersquatting.

b) Defenses to Trade Mark Infringement

The Trade Mark Act of 1994 also provides some defenses to allegations of trade mark infringement:

i. use of a registered trade mark (not infringed by the use of another UK registered trade mark in relation to goods or services for which the latter is registered)[100]

ii. use of a person's own name or address (in accordance with honest practices)

iii. indications concerning the kind, quality, quantity, intended purpose or other characteristics

iv. use necessary to indicate the intended purpose of a product or service

[98] See Brazell, *supra* at 68.
[99] See Brazell, *supra* at 55. citing: TMA 1994, s. 10(4)
[100] Legislation.gov.uk. 2014. Trade Marks Act 1994, s. 11(1). [online] Available at: http://www.legislation.gov.uk/ukpga/1994/26/section/11 [Accessed: 28 Feb 2014].

v. use of an earlier right in a locality[101]

2.5 German Trademark Law

Unlike the US and UK, Germany is a civil law system. Rather than a system based on common law and building precedent through case law, civil law systems govern solely by statute. In the context of trademark law however, this difference in system is not a big issue because, like both the US and UK, Germany has a statute that governs trademark law. Like the UK, Germany is also a member of the EU, and in 1994, instituted the German Trademark Act ("markengesetz") to comply with the EU Trademarks Directive.[102]

Similar to the United States and UK, the purpose of trademark law in Germany is to protect consumers from confusion and owners of marks against others abusing the mark. Similar to the US, but unlike the UK, the MarkenG protects both registered and unregistered trademark holders. The unregistered holder must show that the mark "has acquired prominence in trade circles by their use, or are well known within the meaning of article 6 of the Paris Convention..".[103]

It is worth noting here that the German law in regard to when a holder would be entitled to trademark protection is much the same as the Community Trademarks due to its complying with Community Trademark Directive.

The German Trademark Act defines trademark as:

> "All signs, particularly words including personal names, designs, letters, numerals, sound marks, three-dimensional designs, the shape of goods or of their

[101] Legislation.gov.uk. 2014. Trade Marks Act 1994. [online] Available at: http://www.legislation.gov.uk/ukpga/1994/26/section/11 [Accessed: 28 Feb 2014].
[102] Stegmaier, B. *German and European Trademark Law Trademark Law at Millennium's Turn: Part Six: Trademarks in the International Arena: Comparative Law*433 (1998)
[103] See Stegmaier, at 434.

packaging, as well as other wrapping, including colours and colour combinations, may be protected as trade marks if they are capable of distinguishing the goods or services of one enterprise from those of other enterprises".[104]

a) Elements of a Trademark Infringement Action

The MarkenG states the following would be grounds for an infringement action:

• using a sign which is identical to the trade mark for goods or services which are identical to those for which it enjoys protection,

• using a sign if the likelihood of confusion exists for the public because of the identity or similarity of the sign to the trade mark and the identity or similarity of the goods or services covered by the trade mark and the sign, including the likelihood of association with the trade mark, or

• using a sign identical with or similar to the trade mark for goods or services which are not similar to those for which the trade mark enjoys protection if the trade mark is a trade mark which has a reputation in this country and the use of the sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark which has a reputation.[105]

Similar to UK, the key act to consider is "in the course of trade". The MarkenG provides some instances of what would be considered "in the course of trade" such as:

• to affix the sign to goods or their wrappings or packaging,

• to offer goods under the sign, to put them on the market, or to stock them for the above purposes,

• to offer or provide services under the sign,

[104] MarkenG §3(1)
[105] MarkenG §14(2)

• to import or export goods under the sign,

• to use the sign in business papers or in advertising.[106]

b) Defenses to Trademark Infringement Action

The MarkenG provides a few defenses that can be asserted by one defending a trademark infringement action. The defending third party may assert (with some provisos) the following:

• lapse[107]

• forfeiture of rights[108]

• Exclusion of rights if the registration of a trade mark with younger seniority is definitive[109]

• Use of names and descriptive indications, spare parts business[110]; and

• Exhaustion[111]

Now that the groundwork has been laid for the rules concerning domain name infringement and trademark law/infringement, it is time to discuss cybersquatting.

[106] MarkenG §14(3)
[107] MarkenG §20
[108] MarkenG §21
[109] MarkenG §22
[110] MarkenG §23
[111] MarkenG §24

Chapter 3: Cybersquatting

Introduction: In the previous sections, I discussed domain names and trademarks. In this section, I will be examining the relationship between domain names and trademarks in the context of cybersquatting. I will start by defining (or attempting to define) cybersquatting, its history up to its current status, discussing the interplay between cybersquatting/domain names and statutes and case law in different country jurisdictions.

3.1 Cybersquatting Definition

Oxford English Dictionary defines cybersquatting as:

"The practice of registering names, especially well-known company or brand names, as Internet domains, in the hope of reselling them at a profit".[112]

3.2 History and issues

Cybersquatting is a form of passing off which occurs on the Internet.[113] As explained in above in section 1.1.2, domain names are simply the human readable address for directing people to the proper address online. Cybersquatting began in the early to mid 1990's after the Internet became commercialized. However, most companies did not realize the massive commercial potential of the Internet initially, and consequently, did not register their companies as domain names. The result of this was that industrious types began registering domain names online that were third parties' trademarks. This was not illegal at the time as domain name registers were

[112] Oxforddictionaries.com. 2014. cybersquatting: definition of cybersquatting in Oxford dictionary (British & World English). [online] Available at: http://www.oxforddictionaries.com/definition/english/cybersquatting [Accessed: 5 Mar 2014].
[113] Duncan Spiers, Intellectual Property Law Essentials 73 (Dundee Univ. Press 2009).

constructed on a first come, first served basis.[114] Further, the applicant was not required to provide any evidence of an association with the name.[115]

However, this creates a problem for the trademark owner as the domain name registrant has rights to the name worldwide. The trademark owner is thus effectively barred from registering their own mark because unlike trademarks, where more than one person can register a trademark depending on their location in the world, only one person is entitled to use a domain name. There was a veritable "gold rush" on registering domain names associated with trademarks of well known companies with the intent to sell back the name to the company for a tidy profit when the company goes to register its name and realizes it is already registered.

Throughout the 1990's there were ever-increasing instances of cybersquatting.[116] It became such a big problem that the US Congress had a meeting on 22 July 1999 to discuss the problem and solutions.[117] Congress concluded from the meeting that Internet commerce was drastically increasing, to the tune of 64.8 billion dollars, and cybersquatting had already caused extensive damage to the industry, stating: cybersquatting "undermines consumer confidence, discourages Internet use, and destroys the value of established brand names and trademarks".[118]

The result of Congress' meeting was the Anti-Cybersquatting Consumer Protection Act, which was the first act of its kind in the world to deal with cybersquatting. The Act spurred on the need for the world to develop a system for dealing with cybersquatting.

Below I will provide an illustration of a typical instance of cybersquatting before continuing with the examination of cybersquatting laws in the US, UK and Germany.

[114]See Cornish and Llewelyn, *supra* at 863.
[115]See Lindsay, *supra* at 96.
[116]SykinWyncot,*Domain Name Abuse*, 29 Int'l Prop Newsletter 2 (2006).
[117] Hearing before the Committee on the Judiciary United States Senate Serial No. J-106-39
[118] Hearing before the Committee on the Judiciary United States Senate Serial No. J-106-39

3.2.1 A typical cybersquatting case

A cybersquatter takes advantage of the confusion that arises from a consumer not knowing that a trademark or well known name is not the same thing as a domain name. The typical cybersquatter would register a domain like walmart.com knowing that most people will go online and search for Walmart's site using a search of "walmart.com" expecting it to be associated with Walmart. Of course, the site was actually registered to the cybersquatter and generally, the cybersquatter would have several methods of making money off his registration.

The cybersquatter can use the well known name to direct traffic to his site, thus taking advantage of the large volume of traffic searching for Walmart.com. Additionally, the cybersquatter, in an action somewhat akin to extortion, will then demand a payment from Walmart for the domain name. If the payment is not made, the cybersquatter will then typically post content of questionable subject matter on the walmart.com domain name, resulting in a diminishment of Walmart's good name with the public. Furthermore, a cybersquatter may engage in slander of a world-wide brand. A classic example of this is Dennis Toppen, who reserved hundreds of well known names in the 1990's and then tried to sell them to the rightful trademark owner.[119]

3.3 US Cybersquatting Law

3.3.1 Anti-cybersquatting Consumer Protection Act of 1999 ("ACPA")

As stated above, the US Congress found the great need to enact a law to deal with cybersquatting due to the increasing importance of Internet commerce to the national economy

[119]Jennifer Golinveaux, *What's in a Domain Name: Is Cybersquatting Trademark Dilution,* 33 U. of San Francisco L. Rev. 641 (1999). Also see: Panavision v. Toeppen, 945 F. Supp 1296

and to protect trademark owner rights. Thus, they enacted section 43(d) of the Lanham Act in 1999.

The ACPA defines cybersquatting as:

the registration or use of a trade mark as a domain name in bad faith with an intention to profit from the mark.[120]

3.3.2 Elements of a Cybersquatting Claim

The ACPA gives an owner of a trademark a cause of action against one who registers a mark in bad faith with the intent to profit when a domain name is:

1) identical or confusingly similar to a mark that was distinctive at the time the defendant's domain name was registered; or
2) identical or confusingly similar to, or dilutive of, a mark that was famous at the time the defendant's domain name was registered.[121]

Thus, in order to assert a trademark claim under the ACPA, an owner must prove:

1) it has a valid trademark entitled to protection;
2) its mark is distinctive or famous;
3) the defendant's domain name is identical or confusingly similar to, or in the case of famous marks, dilutive of, the owner's mark; and
4) the defendant used, registered, or trafficked in the domain name;
5) with a bad faith intent to profit.[122]

It is important to note that the 'confusingly similar' element of this act is analyzed differently

[120] 15 USC §1125(d)
[121] See Lafrance, *supra* at 238.
[122] See Lafrance, *supra* at 140.

from the traditional 'likelihood of confusion' trademark analysis.[123] The ACPA only looks at the senior user's mark and the junior user's domain name.[124] In examining the 'bad faith intent to profit', the ACPA offers the following list of factors (non-exhaustive) to consider:

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

[123]See Lafrance, *supra* at 238.
[124]See Lafrance, *supra* at 238.

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.[125]

3.3.3 Defense to a Cybersquatting Claim

The Act states that bad faith shall not be found in:

'any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful'.[126]

It should also be noted that the courts have not come up with a consensus on how to treat domain name cases. Courts have difficulty due to the complex nature of wanting to protect free trade and freedom of expression, while also needing to protect the rights of trademark owners. For instance, some courts have held that there are no trademark violations on parody sites[127] or sites using trademarks, but are not used in commerce but rather, to express ideas and thus lead to First Amendment issues.[128] Thus here are some instances of defenses to a cybersquatting claim.

3.4 United Kingdom Cybersquatting Law

Unlike the United States, the UK has not specifically enacted a law for cybersquatting. The English Courts have dealt with cybersquatting through the 1994 Trademarks Act and through the cases. The UK approach to dealing with cybersquatting was established in the

[125] 15 U.S.C. §1125 (b)(i)
[126] 15 U.S.C. §1125 (b)(ii)
[127] Utah Lighthouse Ministry, 527 F.3d at 105
[128] LucasFilm, Ltd. v. High Frontier, 622 F. Supp. 931, 934

landmark English case on cybersquatting is British Telecommunications Plc v One in a Million Ltd.[129]

In this case, the defendant(s) had registered the following domain names: ladbrokes.com; sainsbury.com; sainsburys.com; marksandspencer.com; cellnet.net; bt.org; virgin.org; marksandspencer.co.uk; britishtelecom.co.uk; britishtelecom.net; and britishtelecom.com. The Court noted at the time that there was no central authority for the Internet and struggled to determine how to decide the case due to the difficulties in dealing with cybersquatting within the trade mark law framework. Namely, the issue that the defendants had not used the domain names in the course of trade in connection with goods or services, but had merely registered the domain names.

The Court eventually conducted a 'passing off' trademark infringement analysis under 10(3), stating:

"the appellants seek to sell the domain names which are confusingly similar to registered trade marks. The domain names indicate origin. That is the purpose for while they were registered. Further they will be used in relation to the services provided by the registrant who trades in domain names". The Court also noted:

'There is only one possible reason why anyone who was not part of the Marks & Spencer Plc group should wish to use such a domain address, and that is to pass himself off as part of that group or his products of as theirs'.

Thus here, we see that in the UK, if one can show a pattern of registering domain names for the purpose of simply parking them or using them to divert traffic to the cybersquatter site, a remedy under 'passing off' may be available. However, it is clear based on classical trademark

[129] 1998 FSR 265

infringement elements, that the English courts had to really stretch to fit cybersquatting claims into them.

For instance, the argument that simply registering a domain name and then parking it would not seem to be use in the course of trade as one is selling or buying anything. However, it is clear that English courts considered the policy implications of letting cybersquatting cases go unpunished, i.e.; the economic harm and social costs incurred by rightful trademark owners, and then determined that they would squeeze cybersquatting into traditional trademark law. It is clear though at this point, the One-in-a-Million analysis is the standard British case by which cybersquatting claims are resolved.

3.5 Germany Cybersquatting Law

Similar to the United Kingdom, Germany has not passed a specific statute to cover cybersquatting claims. Also like the United Kingdom, German courts typically handle cybersquatting cases through the trade mark law principles. (specifically under the 1995 Trade Mark Act, the previously mentioned "MarkenG").[130] Thus, typically in Germany the elements laid out for trade mark law above in section 2.5 will be applied to a domain name infringement case.

Furthermore, protection may be available under section 12 of the German Civil Code (BGB) in cases where "a company's business function is affected as a result of the use of its mark outside its normal operational area".[131]

Additionally, a party seeking protection could assert a claim under the German Act against unfair competition (Gesetzgegen den unlauterenWettbewerb ("UWG").[132] However,

[130]See Pechan, *supra* at 167.
[131]See Pechan, *supra* at 167. Stating: "This occurs whenever the company mark is used outside its normal commercial activity or outside a company's branch and, therefore, is beyond any likelihood of confusion".

domain name claims under this Act have been minimal to date because generally aspects of competition are already covered by trade mark laws.

Dr. Lambert Pechan further states that "In addition to competition law and trade mark law, the general provisions of civil are used to fill gaps in protection, particularly the general prohibition against intentional damage contrary to public policy under section 826 of the German Civil Code".[133]

It should also be noted that Germany has also implemented the Trade Mark Harmonization Directive, and thus is an avenue for complainants to consider.

[132]See Pechan, *supra* at 167.
[133]See Pechan, *supra* at 167.

Chapter Four: Remedies

Introduction: Cybercrime has been roughly doubling each year since 2003[134] and therefore, it became vitally important to provide protection for real world holders of marks for violations in the virtual world of the Internet by cybersquatters. Generally, those alleging cybersquatting violations have two remedies: go through the ICANN-instituted UDRP process, with dispute resolution providers hearing their grievances, or go to the national courts. In this section I will be discussing each of the above remedies in relation to cybersquatting and domain name infringement.

4.1 Dispute Resolution Outside of Courts

4.1.1 Contractual Basis for Mandatory Dispute Resolution

ICANN (through the UDRP) offers expedited dispute resolution proceedings for holders of trademarks to contest abusive registrations of domain names. When a domain name registrant registers a domain name through ICANN, a provision incorporated by reference in every registration agreement provides that there are mandatory administrative proceedings for particular classes of disputes. The ICANN rules state that mandatory proceedings apply when:

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

[134]Reid Goldsborough, *Cybersquatting and Its Possible Remedies,* 23 (38) 9 (2009).

(iii) your domain name has been registered and is being used in bad faith.[135]

Once a claim is submitted to ICANN, they provide a list of approved dispute service providers to choose from. Currently, there are five approved providers on the ICANN site:

• Asian Domain Name Dispute Resolution Center ("ADNRC")

• National Arbitration Forum ("NAF")

• WIPO

• the Czech Arbitration Court Arbitration for Internet Disputes ("CAC")

• Arab Center for Domain Name Dispute Resolution ("ACDR").[136]

The service providers employ panelists that are experts in trademark law and internet issues.[137] Now, I will look at the UDRP remedy and examine some of the benefits and drawbacks of this process.

4.1.2 Uniform Dispute Resolution Policy (UDRP)

I. Necessary Elements to Prove under UDRP

When a registrant registers a website through ICANN, he/she is then contractually obligated to participate in the UDRP process. This is a contractual obligation upon registering for the domain name.[138] A complainant submitting a claim to UDRP must assert the following elements

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

[135] Icann.org. Uniform Domain Name Dispute Resolution Policy (2014) | ICANN. [online] Available at: http://www.icann.org/en/help/dndr/udrp/policy [Accessed: 10 Mar 2014].
[136] Icann.org. List of Approved Dispute Resolution Service Providers (2014) | ICANN. [online] Available at: http://www.icann.org/en/help/dndr/udrp/providers [Accessed: 10 Mar 2014].
[137] See Wright, *supra* at 195.
[138] See Lindsay, *supra* at 103.

(iii) your domain name has been registered and is being used in bad faith.[139]

The UDRP Rules continue, stating: for the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

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

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

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

(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.[140]

It would appear here that any of the evidence of presented would be sufficient for a finding of bad faith, and thus, a decision ordering removal or destruction of the domain name from the Internet.

[139] http://www.icann.org/en/help/dndr/udrp/policy (paragraph 4a)
[140] http://www.icann.org/en/help/dndr/udrp/policy (paragraph 4(a)(iii)

In the UDRP procedure, the burden of proof is on the complainant, who must prove each of the three elements exists. The standard of proof for elements one and three is 'preponderance of evidence'.[141] A preponderance of evidence means 'a balance of probabilities' and is usually understood to mean a bit above 50%.[142] Thus, the elements would be proved if the complainant established they were more likely than not. In regard to the second element, the UDRP requires the complainant to establish that the respondent has no legitimate interests or rights in a domain name, which would require respondent to establish a negative.[143] Thus, previous panel decisions have held that only a prima facie case be made by complainant, and if successful, the burden of proof then shifts to the respondent.[144] In discussing evidence, it is important to note that UDRP paragraph 15(a) gives the Panel very broad discretion in the weight it gives evidence.[145] This is an issue because, this broad discretion has lead to different standards being applied by different panels to determine the weight of evidence presented.

Furthermore, the UDRP has not implemented a formal doctrine of stare dccisis.[146] The combination of differing standards and no stare decisis has occasionally led to inconsistent UDRP results. However, panels of the UDRP understand that it is important that decisions in case involving similar circumstances should be decided in a similar manner. This ensures that participants feel that the system is operating in a fair, effective and predictable manner.[147] Thus, where a majority consensus view seems to have materialized in case precedent, a UDRP panel will generally apply the majority view in the interest of fairness and consistency.

[141]See Lindsay, *supra* at 154.
[142]Dominique Demougin& Claude Fluet. *Preponderance of Evidence,* 50 (4) Eur. Econ. Rev.964 (2006).
[143]See Lindsay, *supra* at 154.
[144]See Lindsay, *supra* at 154.
[145]See Lindsay, *supra* at 155.
[146]See Lindsay, *supra* at 154.Note: could also cite here: Societe des Hotels Meridien SA v United States of Moronica, D2000-0405 (27 June 2000) ('the principle of state decisis does not apply in these proceedings')
[147] WIPO, WIPO Overview of WIPO panel Views on Selected UDRP Question (23 Mar 2005) available at http://www.wipo.int/amc/en/domains/search/overview/index.html

Now that we have examined the elements that must be proved by the complainant, it is time to examine some defenses that may be asserted.

II. Defenses under UDRP

To begin with, let us strike the defenses which are not available under the UDRP. Equitable defenses, such as laches, waiver, forfeiture and unjust enrichment have been rejected by a majority of UDRP panels.[148] UDRP Rules state the following as acceptable evidence to present as a defense:

'Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.'[149]

Thus, it would appear that any respondent that can negate one of the three elements utilizing one of these methods of defense would be able to prevail in a UDRP panel decision.

[148] See Lindsay, *supra* at 155.

[149] http://www.icann.org/en/help/dndr/udrp/policy (paragraph 4c)

4.1.3 The Benefits of Dispute Resolution Provider

According to the WIPO site, the benefits of going through a dispute resolution service provider as opposed to the national court system are "rapid resolution, its cost effective, there is international jurisdiction, simplicity of procedure and availability of appellate process".[150] For instance, the typical time from filing to decision in the UDRP is approximately sixty days.[151] This is considerably faster than a typical federal court case, which can run the course of years. Furthermore, the process can be considerably cheaper than litigating the matter in a court. A dispute resolution panel of three typically costs approximately $4,000 US dollars.[152] Contrast that to the fact that an average attorney litigating a federal matter will typically charge a $10,000 retainer up front and one can see there are clear benefits to resolving a claim through the UDRP process.

Additionally, it is clear that UDRP decisions having effect world-wide is a huge benefit because you don't run into problems with jurisdiction and service of process. Another added benefit to the UDRP process is that a complainant failing to obtain redress for his grievance can still pursue the matter through the national courts. Thus, this could be construed to be an added benefit. However, there are drawbacks to proceeding in a claim under the UDRP process.

[150] Wipo.int. Benefits of the UDRP (2014). [online] Available at: http://www.wipo.int/amc/en/events/conferences/2000/presentations/bernstein/sld002.html [Accessed: 10 Mar 2014].
[151] Cliff Kuehn,*3 Advantages of UDRP Over Litigation in Cybersquatting Situations* (2011). [online] Available at: http://trademarkcopyrightlaw.wordpress.com/2011/07/25/3-advantages-of-udrp-over-litigation-in-cybersquatting-situations/ [Accessed: 10 Mar 2014].
[152] Cliff Kuehn, 3 Advantages of UDRP Over Litigation in Cybersquatting Situations (2011). [online] Available at: http://trademarkcopyrightlaw.wordpress.com/2011/07/25/3-advantages-of-udrp-over-litigation-in-cybersquatting-situations/ [Accessed: 10 Mar 2014].

4.1.4 The Drawbacks of the UDRP Process Dispute Resolution Provider

There a few drawbacks to pursuing a remedy through the UDRP Process. The first one that usually comes up in criticisms of the UDRP is the limited remedy available.[153] As previously discussed in section, UDRP only allows for the cancellation or transfer of the offending domain name. Furthermore, monetary damages are not available, nor is injunctive relief.[154]

Additionally, as previously noted, UDRP panelists are not required to follow the doctrine of stare decisis (following case precedents).[155] This has led in the past to allegations of inconsistency in the decisions of the court, however a more recent study has shown that three member panels seemed to increase stability in decisions.[156]

The last drawback has already been discussed also as a benefit, that being, one can still pursue the matter in a national court if they don't feel that UDRP process was proper, final and binding. As Sarah Silbert notes: "Complainants who initiate UDRP arbitration must agree to submit to a court of mutual jurisdiction in the event the respondent challenges the panel's decision".[157]

The reason this is a drawback is because it generally shows the lack of real precedential power of the UDRP process. It does not say much for the UDRP that they can issue a decision that is regarded by one party as a final adjudication of the matter, and then the other party doesn't like the result, and so goes to the national court system, who then overrule the UDRP Panel.[158]

[153]See Wright, *supra* at 198.
[154]Diane L. Kilpatrick, *ICANN Dispute Resolution Vs. Anti-cybersquatting Consumer Protection Act Remedies: Which Makes More "Cents" for the Clients?*, 2 Hous. Bus. & Tax L. J. 299 (2002).
[155]See Wright, *supra* at 195.
[156]See Wright, *supra* at 195.
[157]Sarah Silbert, *Using a UDRP Action to Prevent Infringing Uses of Domain Names,* 2008 Los Angeles Lawyer 10 (2008) *available at*http://www.lacba.org/Files/LAL/Vol30No11/2454.pdf.
[158]Jenny Ng, The Domain Name Registration System26 (Routledge 2012).

In essence, one can potentially "have their cake, and eat it too" and consequently, may lead to feelings of injustice or instability in the UDRP process by certain participants.

In examining the benefits and drawbacks of the UDRP process, it is clear that these are important factors to consider when filing a claim as it could potentially save, or cost a lot of money and time. In the next section, I will discuss the national judicial systems as a remedy for cybersquatting/domain name infringement claims.

4.2 National Jurisdiction

4.2.1 The United States(U.S.)

Benefits:

As previously discussed, in the US you can file a claim through the UDRP Process or you can file through the State or Federal system. Under the UDRP process, one is of course limited to the remedy of cancellation or transfer of the offending domain name. However, a benefit of the US court system is that it offers more remedies than the UDRP such as injunction and monetary damages in addition to the UDRP remedies.

Drawbacks:

There are some drawbacks to filing in the national court system. The availability of more remedies often means more time in the court room litigating. The average duration for court cases was 8.1 months compared to 10 weeks for UDRP.[159] Furthermore, a big issue with filing in the national courts will be jurisdiction. In order to properly serve bring a party before the court, the court must first obtain jurisdiction.[160] This can present problems in the context of the internet

[159]See Wright, *supra* at 198.

[160] Andrew J. Grotto, *Due Process and In Rem Jurisdiction Under the Anti-Cybersquatting Consumer Protection Act*,2 Colum. Sci. & Tech. L. Rev. 3. (2001)

as the complainant may be bringing suit in the US, but the domain name was registered in Taiwan.

These potential benefits and drawbacks should be carefully considered by a party considering whether to bring a claim before the US court system, or go through the UDRP process.

4.2.2 United Kingdom (U.K.)

In the United Kingdom, the avenues available for remedy are through the Trade Mark Act 1994 and consequently, through the article 5(1)(a) of the trade marks Directive of the European Union. [161] Similar to the US, one may also file through the UDRP for redress. The benefits and drawbacks in the UK are very similar to the US. UDRP is less expensive and saves time, however the remedy is limited. Litigating through the national courts provides more remedies, but also will generally cost more in time and money.

4.2.3 Germany

Similar to the US and the UK, one can seek redress in Germany through the UDRP. Also similar to the UK, one may pursue a remedy under the national courts through their Trade Mark Act and vis a vis through article 5(1)(a) of the trade marks directive.[162] The German courts have offered remedies such as injunctions on use of the domain name[163] however, it should be noted that there is normally no right to cancellation or conveyance of a domain name in Germany under trade mark protection[164], however this remedy might be available based on a claim under

[161]David Bainbridge & Claire Howell, Intellectual Property Law 175 (Pearson Longman 2011).
[162]See Pechan, *supra* at 167.
[163]See Pechan, *supra* at 169.
[164]See Pechan, *supra* at 167.

competition law.[165] Thus in Germany, it may be advantageous to go through UDRP first to determine if one can get a satisfactory result. If not, then one can always file with the German courts per UDRP rules.

Having considered the available remedies under UDRP and national system, it is now time to determine whether there are better solutions than the current system in place.

[165]See Pechan, *supra* at 173.

Chapter 5: Solutions

Introduction: In this section, I will give a very brief introduction of the concept of statehood and then discuss modern jurisdictional issues with cybersquatting and then offer possible solutions to the problems.

5.1 Statehood and Jurisdictional Issues

The concept of statehood and national boundaries is a relatively new one in the annals of time, dating from the Treaty of Westphalia in 1648. This Treaty ushered in the concept of the sovereign state as opposed to vast empires. It established the notion that a sovereign state should not interfere in the affairs of other sovereign states and was the first treaty to in some sense, establish international order.[166] This understanding of statehood and sovereign territories and jurisdictions extends to today. For instance, there are currently 195 independent states in the world.[167]

In the context of the Internet and cybersquatting, this is a huge implication because it means essentially that there are 195 potential jurisdictions with different laws and regulations. When one considers that jurisdiction is difficult enough to establish with acts occurring in the physical world, one begins to see the slippery slope to establishing jurisdiction for acts occurring in the virtual world where information travels across states at dizzying speeds.

Dr. Joanna Kulesza considers this issue, noting that the Internet is "aterritorial".[168] Dr. Kulesza, quoting S. Roseanne defines "Aterritorial" to mean:

[166]Steven Pinker, The Better Angels of Our Nature283 (Viking 2011).
[167] U.S. Department of State. Independent States in the World (2014). [online] Available at: http://www.state.gov/s/inr/rls/4250.htm [Accessed: 11 Mar 2014].
[168]Joanna Kulesza , *Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace*,2008 III GigaNetSymp. Working Paper 1 (2008). A*vailable at:* SSRN: http://ssrn.com/abstract=1445452 or http://dx.doi.org/10.2139/ssrn.1445452.

> "Unlike other spaces, cyberspace is invisible, unidentifiable, irrefragable, and cannot be felt or identified in any way: it has no known natural characteristics. It is simply there, and used by electromagnetic impulses made by human beings. The law can control the use that human beings put to it, and its use can be a subject of agreement".[169]

When dealing with cybersquatting and the limitless boundaries of the Internet set against the very definite issue of real-world boundaries and jurisdiction of the Nation State, the issue become akin to a virtual Gordian knot. This jurisdictional problem is clear especially when considering the principle of territoriality.

Max Planck Institute describes it thusly:

> "According to the principle of territoriality, the scope of protection of an IP right is limited to the territory of the State where the right is granted. Thus different, and from each other independent, national and regional protection rights which are subject to different legal regimes may exist alongside each other on the same immaterial good. The principle of territoriality forms the basis for both national and regional IP laws as well as multilateral conventions on intellectual property protection and can therefore be considered an internationally recognised principle structuring the protection of IP rights".[170]

[169] See Kulesza, *supra* at 1.

[170] Ip.mpg.de. 2014. Max Planck Institute for Innovation and Competition- The Concept of Territoriality and its Impact on Intellectual Property. [online] Available at: http://www.ip.mpg.de/en/pub/research_teaching/ip/main_areas/concept_of_territoriality.cfm [Accessed: 11 Mar 2014].

Max Planck further notes: "in the attempts to justify territoriality, one observes a shift from a strict understanding of sovereignty toward an emphasis on the economic, social and socio-political dimension of IP law, which is based on a locally determined balance of interests".[171]

Even a cursory examination of the definitions of the principle of territoriality and the aterritoriality of the internet, side by side evidences jurisdictional issues. Namely, that due to the reach of the Internet, the principle of territoriality and sovereignty of states are not sufficient for enforcing IP rights and bringing infringers to justice. With this in mind, I would like to examine solutions to the issue.

5.2 Solutions to Cybersquatting and Jurisdictional Issues

In examining solutions it important to determine whether one thinks the problems Internet can be solved through existing law and framework, (unilateralists)[172] or that the Internet is an entirely new phenomenon and thus new laws are needed (multilateralists).[173] In looking at previously discussed sections in this paper on the development of the Internet, and the subsequent development of trouble fitting cybersquatting/domain name infringement cases into existing law, it seems clear that it would be difficult to solve Internet problems with existing law and framework. Furthermore, the rapid speed at which the Internet changes would also seem to necessitate the need for new laws that can adapt to the pace of change.

On the flip side, laws that shift rapidly enough to keep track with the Internet would produce potential instability, thus inhibiting economic and intellectual growth of the Internet. If one cannot be sure of what the law was, is or will be, then that would be an ocean of chaos.

[171] Ip.mpg.de. 2014. Max Planck Institute for Innovation and Competition- The Concept of Territoriality and its Impact on Intellectual Property. [online] Available at: http://www.ip.mpg.de/en/pub/research_teaching/ip/main_areas/concept_of_territoriality.cfm [Accessed: 11 Mar 2014].
[172] See Kulesza, *supra* at 15.
[173] See Kulesza, *supra* at 15.

In an effort to be proactive in the institution of new rules and international cooperation/regulation of the Internet, the United Nations instituted the Working Group on Internet Governance ("WGIG") in 2005.[174] The report made the point that regulation and governance of the Internet must encompass the private sector, the governmental sector and civil sector.[175]

This cooperation against cross sectors will be instrumental in shaping the future of Internet regulation and laws relating to issues such as cybersquatting because of the far reaching, extra-territorial reach of the Internet. Neither one country, nor even twenty countries or actors will be able to resolve the current law and regulation issues of the Internet. A consensus will be necessary to achieve the regulations necessary to combat issues like cybersquatting. Like an international treaty, a consensus will be difficult to obtain if some actors feel like they are not a viable part of the solution and are not allowed to weigh in on governance solutions.

Dr. Kulesza, citing the WGIG report notes that:

"Report sets the minimum standards for such an international exchange:

• No single Government should have a pre-eminent role in relation to international Internet governance.

• The organizational form for the governance function will be multilateral, transparent and democratic, with the full involvement of Governments, the private sector, civil society and international organizations.

• The organizational form for the governance function will involve all stakeholders and relevant intergovernmental and international organizations within their respective roles".[176]

[174] United Nations Working Group on Internet Governance, Report, UN WGIG, 2005, available at: http://www.wgig.org/docs/WGIGREPORT.doc (WGIG Raport).
[175] See Kulesza, *supra* at 18.
[176] See Kulesza, *supra* at 20.

5.2.1 Principles Proposed as Solutions

Dr. Kulesza surveys a few different types of principles bandied about as possible solutions to Internet governance. I will examine some of these and then make a suggestion of my own.

• Effects principle (effective jurisdiction principle). This principle stands for the proposition that a state may take action if online content produces an effect in within their borders.[177]

This principle, while effective in illustrating in which cases states may take action against infringement, is too broad. As we know, one can register a domain name in Florida and the domain name is valid world-wide, and thus producing potential infringement issues in many different jurisdictions. Would governing under this principle be reasonable? It would seem not because one could never take decisive action in starting a business or producing web content because one could not be sure which jurisdiction(s) he may be held accountable. This uncertainty is exactly what we are trying to avoid in installing new Internet governance to provide relief to offenses such as cybersquatting.

• Personality Principle stands for the proposition that the citizenship of an actor would allow a state to regulate their actions concerning Internet issues.[178]

The principle seems like a potentially viable possibility. A German actor registering a domain name in bad faith in Berlin would concretely know that he is exposed to regulation/punishment in Germany. Thus, one would at least have the stability of knowing that he will be subject to laws that he is familiar with, being a citizen of that state.

One issue with this principle might be a case whereby the following occurs. What if Bruno registers a domain name or produces content in Germany which violates no German law,

[177]See Kulesza, *supra* at 12.
[178]See Kulesza, *supra* at 12.

however, it has caused infringement in another State? Is it reasonable for Bruno to expect to be prosecuted in his own State for something that breaks no law in his state? Should Bruno be expedited to State B? Who's law shall be applied if Germany prosecutes Bruno? These are all questions that produce more insecurity for Internet actors rather than less. This scenario is not something that would be a highly unusual situation.

As previously mentioned in this paper, there is no unified Internet law at this juncture of time. Thus, there are numerous divergent laws for different states and the scenario outlined above could actually be quite common. So, the principle is positive in that one would know at least one jurisdiction where accountable. However, the uncertainties could spiral into the same uncertainty in dealing with the effects principle.

• Protective Jurisdiction Principle. This principle stands for the proposition that a state may have jurisdiction where actions which pose a direct threat to a state, or which are "directly targeted" to the state.[179]

This principle seems nice on one hand. An actor can know that if he directs his conduct towards a particular forum or state, he will face potential action there. This is a good thing because it allows states to be proactive in protecting their citizens from harmful cybersquatting or cybercrime action by one committing an intentional act directed to the state or its citizens.

However, this principle still seems over inclusive to me in that if an actor 'poses a direct threat to a state', the state may act. It is conceivable that a state could easily take advantage of this wording to obtain jurisdiction where it has none. After all, one could make the argument that nearly any content uploaded and dispersed online pose a direct threat to a country because there are no borders online. There are no passport checks nor armed guards. As soon as the

[179]See Kulesza, *supra* at 12.

content is uploaded, or the name registered, a direct threat could exist. Thus in effect, nearly giving a state universal jurisdiction, so long as they can justify the infringement posing a direct threat.

Another possible solution is an International Internet Constitution. This solution would need to the participation of nearly all nations around the world due to the Internet reaching into virtually every nation. Ideally, this constitution would lead to a Internet governing body and specific Internet laws enforced by a court, which an actor could be assured of certainty in laws pertaining to the Internet. This leads to a few potential issues:

Firstly, would states be willing to cede sovereignty to an international organization? In regard to this question, there are already real examples of states ceding some sovereignty to an international organization. Some examples are the European Union ("EU") and the United Nations ("UN"). The key in formulating an international organization will be participation of states as the Internet and violations occurring within its spheres are not simply the problem of a few states. Any location in the world that has a connection, from an outpost island in the middle of the Pacific to London, is susceptible to Internet infringement issues. States will need to sign on to the Internet Constitution, and be willing to enforce its provisions.

Secondly, who would enforce the decisions of the governing body and its court? This question might be difficult to answer because of issues ranging from the practical (which state can actually afford to enforce decisions for instance) to the political (will states jockey for lead position in governing the Internet due to the vast power it would bring?). One could write a whole paper on how an Internet Constitution and consequently, a governing body, would be constituted.

In the opinion of this author, the Internet Constitution is the best solution because it would require cooperation amongst states in its formation and would also have the effect of stabilizing issues related to Internet infringement issues such as cybersquatting.

The Internet is a completely new development that current laws are suited for. It is a case of the tortoise and the hare, with cybercrime being the hare and the law being the tortoise. A constitution specifically incepted and formatted to be adaptable enough to fit the ever changing landscape of the Internet would be the best solution for cybersquatting.

Conclusion

Domain name and Trademark infringement and cybersquatting is a very complex subject with lots of moving parts. It would take an academic or statesmen on the level of most gifted Swiss watch maker to take all the moving parts and put them in the proper order to have the system work efficiently and fairly.

Due to the constantly changing nature of the internet, constant vigilance and updates to law will be required. The problem is that laws are slow to change and the Internet is not. It evolves daily at a staggering rate of speed. We need a system of law in conjunction with the internet that can move at the necessary speeds to deal with difficult questions that arise from online infringement.

Until a suitable remedy is enacted, the law will be painfully behind online squatters and cause lots of real world consequences such as loss of goodwill and substantial profits. It appears that for the foreseeable future, domain name infringement actions will continue to be fit into trademark law.

Bibliography

Legal Acts

1998 FSR 265

15 USC §1125(d)

Lanham Act, § 45, 15 USC § 1127.

MarkenG §3(1)

MarkenG §14(2)

MarkenG §14(3)

MarkenG §21

MarkenG §22

MarkenG §23

MarkenG §24

Trade Marks Act 1994 (UK) s 1(1)

Trade Marks Act 1994, s. 10(1)

Trade Marks Act of 1994, s. 10(2)

Committee Meeting

Hearing before the Committee on the Judiciary United States Senate Serial No. J-106-39

United States Cases

LucasFilm, Ltd. v. High Frontier, 622 F. Supp. 931, 934

Panavision v. Toeppen, 945 F. Supp 1296

Utah Lighthouse Ministry, 527 F.3d at 105

United Kingdom Cases

One in a Million

Books

David Bainbridge & Claire Howell, Intellectual Property Law 175 (Pearson Longman 2011).

Lorna Brazell, Intellectual Property Law Handbook 55 (1st ed. The Law Soc'y 2008).

Graham Dutfield& Uma Suthersanen, Global Intellectual Property Law 139 (Edward Elgar Publ'g 2008).

Sheldon W. Halpern, Craig Allen Nard & Kenneth L. Port, Fundamentals of United States Intellectual Property Law 290 (Kluwer Law Int'l 2011).

Mary LaFrance, Understanding Trademark Law 6 (LexisNexis 2009).

Robert C. Lind, Trademark Law 5 (N. Carolina Academic Pr 2006).

David Lindsay, International Domain Name Law (Hart Pub Ltd. 2007).

Duncan Matthews, Globalising Intellectual Property Rights 8 (Routledge 2003).

Jenny Ng, The Domain Name Registration System 26 (Routledge 2012).

Shoen Ono, Overview of Japanese Trademark Law 1 ch.2 (2nd ed. Yuhikaku 1999).

Steven Pinker, The Better Angels of Our Nature 283 (Viking 2011).

W. William Rodolph Cornish & David Llewelyn, Intellectual Property 607 (Sweet & Maxwell 2007).

Duncan Spiers, Intellectual Property Law Essentials 73 (Dundee Univ. Press 2009).

Journals

M. Tariq Banday, *Recent Developments in the Domain Name System*, 31 Int'l J. of Computer Applications, Found. of Computer Sci. 18 (2011).

James E. Darnton, *Coming of Age of the Global Trademark: The Effect of Trips on the Well-Known Marks Exception to the Principle of Territoriality,* 20 (1) The Mich. St. C. of L. Int'l L. Rev. 16 (2011).

Dominique Demougin& Claude Fluet, *Preponderance of Evidence,* 504 Eur. Econ. Rev. 964 (2006).

Catherine R. Easton, *ICANN's Core Principles and the Expansion of Generic Top-level Domain Names* , 20 Int'l J. of L. & Info. Tech. 275 (2012).

Reid Goldsborough, *Cybersquatting and Its Possible Remedies,* 23 Bus. J. (Central New York) 9 (2009).

Jennifer Golinveaux, *What's in a Domain Name: Is Cybersquatting Trademark Dilution,* 33 U. of San Francisco L. Rev. 641 (1999).

Diane L. Kilpatrick, *ICANN Dispute Resolution Vs. Anti-cybersquatting Consumer Protection Act Remedies: Which Makes More "Cents" for the Clients?,* [II] 299 (2002).

Steven Kuehn. http://trademarkcopyrightlaw.wordpress.com/2011/07/25/3-advantages-of-udrp-over-litigation-in-cybersquatting-situations/.*Available att* http://trademarkcopyrightlaw.wordpress.com/2011/07/25/3-advantages-of-udrp-over-litigation-in-cybersquatting-situations/ (last visited Mar. 21, 2014).

Joanna Kulesza , *Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace,* 2008 III GigaNetSymp. Working Paper 1 (2008) *available at*SSRN: http://ssrn.com/abstract=1445452 or http://dx.doi.org/10.2139/ssrn.1445452.

P. V. Mockapetris& K. J. Dunlap, *Development of the Domain Name System,* 18 ACM Computer Comm. Rev. 123 (1988).

Milton Mueller, *The Battle Over Internet Domain Names: Global or National TLDs?,* 22 Telecomm. Pol'y 90 (1998).

Leslie Suzanne Park, *The Primary Trademark Identifier Requirement: A Change to Current Trademark Law,* 2013 Seton Hall L. ERepository 1 (2013).

Lambert Pechan, *Domain Grabbing in Germany: Limitations of Trade Mark Protection and How to Overcome Them,* 7 J. of Intell. Prop. L. &Prac. 166 (2012).

Lisa M. Sharrock, *The Future of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions from Within the UDRP Framework,* 51 Duke L. J. 817 (2001).

Sarah Silbert, *Using a UDRP Action to Prevent Infringing Uses of Domain Names,* 2008 Los Angeles Lawyer 10 (2008) *available at* http://www.lacba.org/Files/LAL/Vol30No11/2454.pdf.

Stegmaier, B. *German and European Trademark Law Trademark Law at Millennium's Turn: Part Six: Trademarks in the International Arena: Comparative Law*433 (1998).

Ian Tollet, *Domain Names and Dispute Resolution,* 23 World Pat. Info. 169 (2001).

Christopher Varas, *Sealing the Cracks: A Proposal to Update the Anti-cybersquatting Regime to Combat Advertising-based Cybersquatting,* 3 J. of Intell. Prop. L. 246, 246-261 (2008).

Steven Wright, *Cybersquatting at the Intersection of Internet Domain Names and Trademark Law,* [14 (1)] IEEE Comm. Surveys & Tutorials 194 (2012).

Sykin Wyncot, *Domain Name Abuse*, 29 Int'l Prop Newsletter 2 (2006).

Online Sources

Ip.mpg.de. 2014. Max Planck Institute for Innovation and Competition- The Concept of Territoriality and its Impact on Intellectual Property. [online] Available at: http://www.ip.mpg.de/en/pub/research_teaching/ip/main_areas/concept_of_territoriality.cfm [Accessed: 25 Feb 2014]

Ipo.gov.uk. 2014. Intellectual Property Office - Infringement, What is trade mark infringement?. [online] Available at: http://www.ipo.gov.uk/types/tm/t-other/t-infringe.htm [Accessed: 27 Feb 2014].

Law.cornell.edu. 2014. Trademark | Wex Legal Dictionary / Encyclopedia | LII / Legal Information

Legislation.gov.uk. 2014. Trade Marks Act 1994, s. 11(1). [online] Available at: http://www.legislation.gov.uk/ukpga/1994/26/section/11 [Accessed: 28 Feb 2014].

Oami.europa.eu. 2014. Who we are. [online] Available at: https://oami.europa.eu/ohimportal/en/who-we-are [Accessed: 26 Feb 2014].

Oxforddictionaries.com. 2014. cybersquatting: definition of cybersquatting in Oxford dictionary (British & World English). [online] Available at: http://www.oxforddictionaries.com/definition/english/cybersquatting [Accessed: 5 Mar 2014].Institute. [online] Available at: http://www.law.cornell.edu/wex/trademark [Accessed: 27 Feb 2014].

Wipo.int. 2014. Inside WIPO. [online] Available at: http://www.wipo.int/about-wipo/en/index.html [Accessed: 26 Feb 2014].

Wipo.int. 2014. WIPO-Administered Treaties: Paris Convention for the Protection of Industrial Property. [online] Available at: http://www.wipo.int/treaties/en/text.jsp?file_id=288514#P174_27991 [Accessed: 26 Feb 2014]. Article 6(3)

Wto.org. 2014. WTO | About the organization. [online] Available at: http://www.wto.org/english/thewto_e/thewto_e.htm [Accessed: 26 Feb 2014].