TONJE RØSTE GULLIKSEN

INTERNATIONAL REGULATION AND PROTECTION OF INTERNETT DOMAIN NAMES AND TRADEMARKS

COMPLEX 1/99
INSTITUTT FOR RETTSINFORMATIKK

Tano-Aschehoug
# TABLE OF CONTENTS

Synopsis................................................................................................................................................... 5  
Jurisdictions.......................................................................................................................................... 8  
Introduction......................................................................................................................................... 9  

1 BACKGROUND ON THE INTERNET........................................................................................................ 11  
1.1. DEFINITION OF THE INTERNET, ITS HISTORY AND TECHNICAL STRUCTURE...... 11  
1.2. THE DIFFERENT USAGES OF THE INTERNET .................................................. 14  
1.3. THE MAIN INTERNET PLAYERS ......................................................................... 16  
1.4. HOW ARE WWW STANDARDS CREATED? ....................................................... 20  

2 WHAT IS A DOMAIN NAME? ............................................................................................................. 22  
2.1. DEFINITIONS ................................................................................................................... 22  
2.2. THE NATURE OF A DOMAIN NAME .......................................................................... 24  
2.2.1. Are domain names property? .............................................................................................. 25  
2.3. THE ALLOCATION OF SECOND-LEVEL DOMAIN NAMES .................................... 29  
2.4. BACKGROUND ON THE PROBLEMS REGARDING SLD NAMES UNDER .COM” .. 32  
2.5. OVERVIEW OF THE MAJOR PROBLEMS REGARDING SLD NAMES ................... 34  

3 BACKGROUND ON TRADEMARKS........................................................................................................ 37  
3.1. DEFINITION .................................................................................................................. 37  
3.2. THE RATIONALE ........................................................................................................... 38  
3.3. EXAMPLES .................................................................................................................... 38  
3.4. THE DIFFERENT TYPES OF TRADEMARKS ............................................................. 39  
3.5. DISTINCTIVENESS ......................................................................................................... 39  
3.6. ACQUISITION OF TRADEMARK RIGHTS ............................................................... 42  
3.6.1. Actual use and registration .......................................................................................... 42  
3.6.2. What kind of use is required to acquire trademark protection? ......................... 44  
3.6.3. Registration of domain names as trademarks ......................................................... 44  
3.7. INTERNATIONAL TRADEMARK FILING AGREEMENTS ........................................... 45  
3.8. TRADEMARK INFRINGEMENT AND DILUTION ......................................................... 46  
3.8.1. Australia ...................................................................................................................... 47  
3.8.2. The United States ......................................................................................................... 49  
3.8.3. The United Kingdom .................................................................................................... 51  
3.9. INTERNATIONAL HARMONISATION OF THE PROTECTION OF WELL-KNOWN TRADEMARKS ................................................................. 52  
3.9.1. The Paris Convention ................................................................................................. 53  
3.9.2. TRIPS ......................................................................................................................... 55
INTERNATIONAL GOVERNANCE OF THE INTERNET

6.1 THE INTERNET CREATES PROBLEMS FOR THE CURRENT DOMESTIC LEGAL SYSTEMS

6.2 THE PROPOSED MODELS FOR INTERNET GOVERNANCE: SELF-REGULATION OR INTERNATIONAL GOVERNANCE?

6.2.1 International organisations

6.2.2 Should the state remain the key international player?

THE CONCLUSION AND SOME FINAL REMARKS

APPENDIX A: The usage of Internet

APPENDIX B: Table of statutes

APPENDIX C: Table of treaties and international agreements

APPENDIX D: Table of cases

APPENDIX E: Glossary

APPENDIX F: Bibliography

APPENDIX G: NSI’s Dispute Policy
INTERNATIONAL REGULATION AND PROTECTION OF
INTERNET DOMAIN NAMES AND TRADEMARKS

SYNOPSIS

The Internet and commerce

The Internet is of increasing importance to commerce. The global scope of the World Wide Web makes the Internet an international marketplace. For businesses, the Internet is an excellent means of advertising and selling their products and services. The Internet congregates the world into one single market and with a small investment a business gets access to this worldwide marketplace. Internet presence gives businesses vast possibilities. With products and services available online, the business can reach virtually everyone. Moreover, the Internet has the benefit of reaching the potential customer at home or at the office. For the consumers, the Internet provides an efficient and fast manner of doing commercial transactions. The World Wide Web is easy to access and provides for the convenience of shopping at home. There is no doubt that the Internet is increasingly important to commerce - this is the new trend and the future of advertising, selling and purchasing products and services.

Internet domain names

One of the reasons for the growing popularity of the Internet among people is the user-friendly manner of searching the World Wide Web. A company’s World Wide Web address commonly consists of its trade name with the addition of “.com”. The part of the World Wide Web (WWW) address after “www” is called the domain name. As a company’s domain name often is its trade name, potential customers find their way through the WWW by browsing, searching and surfing the WWW by domain names. They guess domain names and follow hypertext links to the next destination. The result of this practice is that it is crucial to a company’s Internet exposure to have a domain name similar to its trade name in order to
reach potential customers and successfully selling products and services through the Internet.

**Trademarks**

The importance of having a domain name in cyberspace similar to a trade name in the real world links domain names to trademarks. A company’s trade name is often protected by intellectual property rights, as the trade name often is a registered trademark or servicemark. However, as trademark registration is a national system, several businesses around the world may own the same or similar trademarks and servicemarks. In contrast, as the Internet is global and under one category of domain names (e.g. “.com” for commerce purposes), the domain name must be unique. The main problem in the conflict between domain names and trademarks is that domain names are allocated on a first come-first served basis. Consequently, in the competition between businesses to get their trade name as a part of their WWW address, breach of intellectual property rights have been alleged and trademark infringement and dilution have been used to attack domain name holders already holding the domain name that a particular company wants. The introduction of trademark law into the lawless Internet has not been successful.

**International proposals**

The conflict in the Domain Name System (DNS), where domain name holders and owners of trademarks and other intellectual property rights collide, has lead to the drafting of several proposals at the international level. The proposals attempt to regulate and bring order to the Internet. Consequently, the Internet is facing a transition at the governance level. However, lack of legal authority has lead to the result that these proposals can not fully address the problem.

**The aims and objectives**

This thesis is aimed at examining the above mentioned issues and analysing solutions of the current transitional problems. The main
finding of this thesis is that we need a stable governance system to secure the environment for all Internet users and to find a lasting solution to the current problems. The specific aims of this thesis are to:

* analyse the problems of domain names in general;

* examine the disharmony between domain names and trademarks;

* critically analyse whether contemporary trademark law provides the mechanisms for an effective and feasible solution of domain name conflicts;

* outline the current policies regarding domain name allocation and dispute resolution. The Network Solutions, Inc. (NSI) policy in the United States will be thoroughly examined, and compared and contrasted with the Nominet policy in the United Kingdom and the Melbourne Information Technologies Australia (Melbourne IT) policy in Australia;

* critically analyse why so much more litigation has resulted from the NSI policy than from any other policy;

* discuss the proposal of a cybermark;

* thoroughly examine the Memorandum of Understanding on the generic Top-Level Domain Name Space of the Internet Domain Name System (gTLD-MoU);

* examine whether there should be a system of self-governance or international governance of the Internet;

* analyse whether international organisations, currently existing or not, are suited to set Internet policy; and

* critically evaluate the models for Internet governance and propose a new theory - transgovernmentalism.

The solution

This paper will argue that, in the short term, a temporary system of national policies, such as those utilised by Melbourne IT in Australia
and Uninett in Norway, is feasible. A “hands-off” approach to domain name disputes, where each country’s courts deal with the conflicts, will temporarily be the best solution to the domain name issues. In the long term, however, there needs to be an internationally agreed system of governance of the Internet. As the Internet is in transition from a lawless playground for “cybernauts” and a network used by academics to an international marketplace used by the commercial sector and the citizens in general, there should be a system of effective governance on the Internet. The current system of self-governance will not provide sufficient stability and security in commerce. The Internet needs a policy and legal framework to address the problem of domain names, while taking the interests of all Internet stakeholders into account. International organisations are not able to provide the sufficient enforcement and compliance mechanisms, thus state institutions would provide the sufficient jurisdictional authority. In other words, transgovernmentalism should be encouraged.

**Jurisdictions**

This paper will examine Australian, The United Kingdom (UK) and The United States (US) jurisdictions in particular. The situation of Europe, and the European Union (EU) particularly, will be mentioned in comparison with the common law countries when relevant. The paper will predominantly focus on the situation in the US where the Internet has its origins. The majority of domain name conflicts have occurred there. The UK will be examined because of the important *Prince case*. Australia will be examined because the paper was completed there, and because it is a good example of a hands-off approach to domain name disputes.
Introduction

The present thesis forms the conclusion of a research project on the Internet Domain Name System (DNS), the tensions between domain names and trademarks and the proposals for Internet governance. The Internet is evolving to a full commercial network. With the commercialisation of the Internet, companies brandish their trademarks and claim that domain names have to respect their trademarks. This represents a tremendous change as the DNS was designed as an academic network. The irregularities between domain names and trademarks led to the drafting of several proposals within the Internet community, aimed at creating new solutions.

Methodology

The research carried out was aimed at analysing the current conflicts and examining solutions to the transitional problems the Internet faces. The research primarily consisted of searching the Internet. A considerable part of the relevant material was available online. In order to find recent legal journal articles, CD ROM databases such as the Legal Trac databases were utilised. Legal textbooks were consulted where available and relevant to the topic. Moreover, as an essential part of the subject matter researched evolved as the paper was written, a significant portion of the research consisted of subscribing to three different mailing lists. The participation on the mailing lists involved active discussions with other persons concerned about the future of the Internet. A fourth mailing list, the “gtld-announce”, provided for announcements of new events almost instantaneously. The participation on the mailing lists also resulted in personal email contact with persons involved in the transition process, such as Robert Shaw, Switzerland, advisor at the International Telecommunication Union, and Ellen Rony, USA, co-author of the book “The Domain Name Handbook: High Stakes and Strategies in Cyberspace” forthcoming in January 1998.

Overview of the chapters

In order to achieve the aims of this paper, Chapter 1 will provide a short history of the Internet, outline the technical structure of the Internet and introduce the main Internet players. Chapter 2 will analyse the nature of do-
main names, provide an overview of the domain name allocation policies in Australia, the UK and the US, and examine the background on the conflicts between domain names and trademarks. In Chapter 3 the relevant trademark law will be examined. Then, Chapter 4 will bring the issues identified in Chapters 2 and 3 together and analyse the inconsistencies between domain names and trademarks. Chapter 5 will examine the gTLD-MoU and CORE-MoU proposals. Finally, Chapter 6 will outline the problems the Internet causes for the current domestic legal systems, analyse whether international organisations would be suited to govern the Internet, critically evaluate the proposed models for Internet governance. From these analyses a conclusion will be drawn.
1 BACKGROUND ON THE INTERNET

Aims of chapter 1

The aims of Chapter 1 are to:

* provide a short history of the Internet;
* outline the technical structure of the Internet; and
* provide an introduction to the main Internet players.

It is essential to have an understanding of the origins and technical structures of the Internet and to overview the main Internet players. Thereafter, in Chapter 2, follows an introduction to the domain name issue. In Chapter 3 the relevant trademark law will be examined. After these introductions, Chapter 4 will bring the issues together and analyse the conflicts between domain names and trademarks.

1.1 Definition of the Internet, its history and technical structure

The Internet originated in 1968 in the US experiment called ARPA (Advanced Research Project Agency), and was thus called the ARPANET. The ARPANET was designed to allow vital research and communications to continue even if portions of the network were damaged in a war. Thus it began as a means for the military to communicate even if other forms of communication broke down. The project was sponsored by the US Department of Defense.

---


2 Burk, D.L., “Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks” (1 RICH J.L. & TECH. 1, April 10,
This system of communication became increasingly important to the scientific community as universities began to utilise the Internet for educational purposes. Consequently, the US National Science Foundation (NSF) decided to fund much of the Internet. As the ARPANET evolved far beyond its research origins, it came to be called the “DARPA Internet” in 1972, and finally just the Internet.\(^3\) Eventually, as the benefits of the Internet became better known, some private persons formed the Commercial Internet Exchange (CIX).\(^4\) The CIX sponsored high-speed links for commercial traffic on the Internet. Today, the Internet is frequently and widely used for research, emailing, game playing, reading online news and magazines, advertising, banking, shopping, and other commercial and non-commercial uses.\(^5\)

As mentioned above, the Internet was designed to allow vital research and communications to continue even if portions of the network were damaged in a war. This is possible because the Internet is a giant network, which connects innumerable smaller groups of computer networks. It is thus a network of networks.\(^6\) Each link or node in this web is a computer or a computer site connected together. This global web of linked networks and computers has no centralised storage location, control point or communications channel. The Internet exists and functions as a result of the fact that hundreds of thousands of separate computers and computer networks independently decide to use some standard ways to exchange com-

---


2  Burk, above n. 2.

3  See Burk, above n. 2.

4  Burk, above n. 2.


6  Burk, above n. 2.
communications and information with other computers. The standard way by which computers communicate with each other is known as Internet Protocols (IP). A communication sent over the network of computers travels any number of routes to its destination. Hence if one part of the Internet breaks down, the packet of communication just travels via another route. This is called “packet switching” communications protocol because it allows individual messages to be subdivided into smaller “packets” that are sent independently to the destination, and are then automatically reassembled by the receiving computer. As a result, if computers along the route become overloaded, packets can be re-routed to less loaded computers.

An IP address is a numeric address that indicates the location of a computer on the Internet. It is represented as strings of digits divided into parts, or fields. For example, the library computer at the Australian National University has the numeric address of 150.203.85.3. This address contains a network portion, the IP network address, and a location portion, called the local address. However, Internet users may find it difficult to remember these IP numeric addresses. Consequently, the IP numeric address system has been overlaid with a more user-friendly system of domain names.

As revealed above, there is no centralised control of the Internet. Each computer acts autonomously. Consequently, there is no central authority to govern Internet usage, no one to ask for permission to join the network, and no one to complain to when things go wrong. Moreover, the Internet is a global network, with no territorial...
boundaries. The issue of Internet governance will be examined in Chapter 6.

1.2 The different usages of the Internet

The Internet is probably the most powerful means of communication ever invented. It opened up a “marketplace” of ideas to millions of people around the world for the first time in history.\(^\text{14}\) However, the marketplace is not just for commercial activities. It enables people from different parts of the world to discuss and exchange ideas instantaneously, do research for an academic paper, and even plan a vacation. In this paper, the focus will predominantly be on commercial activity on the World Wide Web.\(^\text{15}\)

The services available via the Internet can roughly be placed in six categories:\(^\text{16}\)

* one-to-one messaging (e.g. email);
* one-to-many messaging (e.g. mailing lists);
* distributed message databases (e.g. newsgroups);
* real time communication (e.g. chat);
* real time remote computer utilisation (e.g. telnet); and
* remote information retrieval (e.g. WWW, Gopher).

Email is a messaging function, which enables the users to send electronic mail to each other. At the end of this century, emailing is likely to be as common as the telephone. It is fast, efficient, inexpensive and convenient. One can email someone from one’s own computer, and the email message will reach the recipient wherever he or she is in the world almost instantaneously.

---


\(^{15}\) See Appendix A for usage patterns of the Internet.

\(^{16}\) ACLU v. Reno, above n. 3 at 7.
The mailing list services send information about particular subjects of interest to people who want to subscribe to the mailing list. People can subscribe to a “listserv” mailing list on a particular topic of interest to them; for example, the mailing lists “domain-policy” and “gtld-discuss”, and then email questions and comments for discussion. The mailing list is closed to non-subscribers.

The newsgroups are open discussions and exchanges on particular topics. However, the users need not subscribe to it in advance, but can access the database at any time like a normal World Wide Web page.

The chat service allows two or more users to type messages to each other that immediately appear on the others’ computer screens. It is thus a sort of instantaneous emailing.

Telnet can be used to access a remote computer; for example, a remote library online catalogue program.

The World Wide Web (WWW) enables users to access information (i.e. a hyper media with text, graphics and sound) over the network. The WWW is thus a global online store of knowledge. In order to view material on the WWW, one needs a browser. The browser translates the material from different formats; for example, the format “html” (hypertext markup language) if the WWW address ends with the letters “html”, or text format if the WWW address ends with “txt”. One needs a special locator to identify a location on the WWW. The locator is called a URL (Uniform Resource Locator). The URL consists of two parts, divided by ://. The first part indicates the type of resource and the second the location of the resource (i.e. “protocol://host/path/filename”). The most common protocol is http (hypertext transfer protocol) where host refers to the domain name, path refers to the directory or directories in which the file is

---

17 Dayal, above n. 9 at 146.
18 Dayal, above n. 9 at 147.
19 Ibid
located, and filename is the name of the file that you actually want.\textsuperscript{20} For example http://www.wipo.org/Internet/domains/.

1.3 The main Internet players

 Linked to the technical structure is the current administrative structure of the Internet. It is important to acquire an overview of the actors that until now have been involved in the standardisation process, maintenance and decision-making process of the Internet.

 As mentioned above, no single entity governs the Internet. The computers and computer networks that make up the Internet are owned by government and public institutions, some are owned by non-profit organisations, and some are privately owned.\textsuperscript{21} In fact, the Internet is not governed, it is co-ordinated. One may simply say that the Internet is run by engineers who voluntarily take their time to program, manage and maintain the Internet.\textsuperscript{22} As a result of the Internet's origins, the bodies which have hitherto played a role in the operation and self-management of the Internet are often of US origin and have a majority, or at least a large number, of US members.\textsuperscript{23} The Internet is built up, administered and governed by various entities, such as:

 1) The US National Science Foundation (NSF)\textsuperscript{24}

 The NSF is an independent US government agency responsible for promoting science and engineering.\textsuperscript{25} It provides support and grants

\begin{itemize}
  \item \textit{Ibid}
  \item \textit{ACLU v Reno, above n. 3 at 4.}
  \item Stoodley, J., “Internet Domain Names and Trade Marks” (1997) 19 European Intellectual Property Review 509 at 509.
  \item Visit http://www.nsf.gov
  \item See http://www.nsf.gov/home/about/start.htm (Accessed 19 October 1997).
\end{itemize}
for research in networking and communications, including NSFNET. The relevant group is the Networking and Communications Research and Infrastructure (NCRI) Division in the Directorate for Computer and Information Science and Engineering (CISE). In 1993, NSF created a new organisation to provide specific Internet services, the InterNIC (Internet Network Information Centre). The InterNIC is a co-operative activity between the National Science Foundation, Network Solutions, Inc. (NSI) and AT&T. AT&T supports directory and database services. NSI sponsors registration services, information and education services, and net scout services. The NSI is presently registering second-level domain names under the top-level domains "com", "org", "net", "gov" and "edu". The NSF contracted with NSI for the processing of domain name applications. The contract is a five-year agreement, which expires on 31 March 1998. NSF obtains some funding by a grant from the NSF and the balance is obtained from domain name registration fees.

2) The Internet Society (ISOC)

The ISOC, a non-profit body established in the US, is, according to its homepage, a "non governmental international organisation for global co-operation and co-ordination for the Internet and its Internetworking technologies and applications".

3) The Internet Assigned Numbers Authority (IANA)

26 Visit http://rs.internic.net
27 Visit InterNIC’s information page at http://rs.internic.net.
28 Visit http://www.netsol.com/
29 NSF Co-operative Agreement No. NCR-9218742 is the 5 year agreement between NSF and NSI for allocation of domain names under "com" and several other TLDs.
30 Frank, above n. 22.
31 Visit http://www.isoc.org
32 See http://www.isoc.org/whatis/index.html
33 Visit http://www.iana.org/iana/
Some Internet standards require administrative implementation in order to allow the Internet to be operational. These include Internet Protocol addresses. The overall responsibility for this work is vested in the IANA, which delegates the actual administration of most functions to other bodies.34 IANA is a sister body to the Internet Society.35 IANA is an “Internet Service” of the High-Performance Computing and Communications (HPCC)36 division of the Information Sciences Institute (ISI), a part of the University of Southern California’s School of Engineering.37 It is chartered by the Internet Society and the Federal Network Council to act as the clearinghouse to assign and co-ordinate the use of numerous Internet protocol parameters.38 According to IANA’s homepage, IANA is “the central co-ordinator for the assignment of unique parameter values for Internet protocols”.39 Consequently, IANA is the overall authority for the Internet addresses (i.e. the “international” TLDs, including the country code “.us”), the domain names and many other parameters used on the Internet.40 The IANA assigned its authority to issue domain names for the TLD names “.com”, “.org”, “.net”, “.gov” and “.edu” to the InterNIC.41

4) The Internet Engineering Task Force (IETF)42 and The Internet Engineering Steering Group (IESG)43

35 Stoodley, above n. 23 at 509.
36 See High-Performance Computing and Communications Division at http://www.isi.edu/div7/
37 See Information Sciences Institute at http://www.isi.edu/
38 See http://www.iana.org/iana/overview.html
39 See http://www.iana.org/iana/overview.html
40 Frank, above n. 22.
41 For information about the contract between NSF and NSI, see above in this chapter.
42 Visit http://www.ietf.org/
43 Visit http://www.ietf.org/iesg.html
As noted above, at the technical and developmental level the Internet is made possible through creation, testing and implementation of Internet Standards. The IETF are the engineers who build those Internet standards. The IETF is a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet". The Internet protocol suite, as defined by the IETF and its steering group (IESG), contains numerous parameters, such as Internet addresses, domain names, autonomous system numbers, protocol numbers, and many others. Thus the IETF takes care of the technical issues that make the Internet run. The IESG handles the internal management of the IETF with IANA as the central co-ordinator. The IETF is principally funded by the US Government.

5) The Internet Architecture Board (IAB)

The IAB is a technical advisory group of the Internet Society. The IAB provides oversight of the architecture for the protocols and procedures used by the Internet and the process used to create Internet standards. Furthermore, the IAB acts as a representative of the interests of the Internet Society in liaison relationships with other organisations concerned with standards and other technical and organisational issues relevant to the Internet.

6) The World Wide Consortium (W3C)

The W3C is another organisation involved in the development of the Internet protocols. The W3C’s stated goal is to set standards that all
WWW developers can follow. The W3C is the guardian of most browser standards (such as html).\textsuperscript{50} It was created in 1994 by Tim Berners-Lee, known as the father of the WWW.

1.4 How are WWW standards created?

Having provided an overview of the organisations involved in the standardisation process on the Internet, the actual process can now be analysed.

Generally, the IETF develops the Internet standards.\textsuperscript{51} The standards are then considered by the IESG, with appeals to the IAB. Finally, they are promulgated by the Internet Society as international standards.\textsuperscript{52} Until now, this process has developed though Request For Comments (RFCs) utilised by the various organisations described above.\textsuperscript{53} The Requests for Comments are a series of notes, started in 1969, about the ARPANET (the predecessor to the Internet).\textsuperscript{54} The notes discuss many aspects of computing and computer communication focusing in networking protocols, procedures, programs, and concepts, but also including meeting notes, opinion, and sometimes humour.\textsuperscript{55} Hence the RFCs are essentially the governing documents

\begin{itemize}
\item \textsuperscript{50} CNET, “Whoever controls the browser controls the Web. But who is that?” [WWW http://www.cnet.com/Content/Features/Dlife/Inside/?dd] (Accessed 1 November 1997).
\item \textsuperscript{52} See http://www.isoc.org/standards/
\item \textsuperscript{53} Suggestions about RFC publication, or submission of material to be considered for publication as an RFC can be sent via email to <rfc-editor@isi.edu>.
\item \textsuperscript{55} E.g. the TLDs “.com”, “.net” and “.org” are defined in RFC 1591 and the DNS is published in RFC 1034 and 1035. See also RFCs 1122 and
\end{itemize}
for the Internet. For example, the specification documents of the
Internet protocol suite, the standards as defined by the IETF and its
steering group (the IESG), are published as RFCs. The RFC Editor
is the publisher of the RFCs and is responsible for the final editorial
review of the documents. The RFC Editor is chartered by the ISOC
and the Federal Network Council (FNC). The RFC Editor is located
at and operated by the Information Sciences Institute (ISI) of the
University of Southern California.

1123. Huitema, C. et al, “Not All RFCs are Standards” [WWW -
2 WHAT IS A DOMAIN NAME?

Aims of chapter 2

The aims of Chapter 2 are to:

* examine the nature of domain names;
* provide an overview of the domain name allocation polices in Australia, the UK and the US; and
* examine the background on the problems regarding domain names and trademarks.

Having considered the Internet, its history, technical and administrative structure, this chapter will focus on domain names. The Internet is currently facing the emergence of a conflict zone with respect to the creation and registration of domain names. To fully understand the domain name issue it is important to examine what a domain name is and how the Domain Name System (DNS) currently works.

2.1 Definitions

Domain names are the plain English references to the IP addresses. Like the IP numeric addresses, the domain names are divided into fields separated by full stops (in the Internet language called “dot”). For example, “www.mcdonalds.com” is a characteristic example of a domain name. As mentioned above, the overlapping system of mnemonic addresses is designed to make the Internet more user-friendly. Consequently, when a domain name is typed into a computer, the Internet software automatically converts the domain name to the numbered address.

A domain name must consist of at least two parts, a “top-level” domain name (TLD), and a “second-level” domain name (SLD). In addition, it may, but need not, have a “third-level” domain name. For example, http://www.core.gtld-mou.org. If one reads from right to left, the fields designate the TLD “org”, the SLD “gtld-mou”, and “core” is the third-level domain. There can be an unlimited number of second-level and third-level domain names in each TLD; how-
ever, there can be only one of each particular second-level domain name in each top-level domain.\textsuperscript{56} Hence the SLD name within one category TLD must be unique. The most widespread use of third-level domain names is within the International Organisation for Standardisation (ISO) 3166 country-code TLD.\textsuperscript{57} In the country-code TLD, the SLDs usually function as categorisers; for example “companyname.com.au”, or “universityname.ac.uk”. Hence in the country-code TLD, the third-level domain name is usually the name that is important to the domain name holder.

Currently, four categories of TLD names exist:

\textbf{(1) ISO 3166 country codes}

There are over 180 country code top-level domains.\textsuperscript{58} A country code TLD is a two-letter abbreviation of the name of the country, for example, “.au” for Australia, “.ca” for Canada, “.no” for Norway and so on. Each country governs its country code TLD, hence the policies may differ from country to country.

\textbf{(2) “.mil”, “.edu”, “.gov”}

There are three TLDs that are reserved for the military, educational institutions and governmental agencies. These TLDs can only be utilised by the US alone, as historical anomalies from the time when the US was the only country utilising the Internet.

\textbf{(3) “.com”, “.org”, “.net”}

\textsuperscript{56} WIPO, “Issues relating to trademarks and Internet domain names” [WWW http://www.wipo.org/eng/Internet/domains/tdn/cm/cm_i_2.htm] (Accessed 22 July 1997).

\textsuperscript{57} The International Organisation for Standardisation (ISO) is a worldwide federation of national standards bodies from some 100 countries, one from each country. ISO’s work results in international agreements which are published as International Standards. See “Introduction to ISO” [WWW - http://www.iso.ch/infoe/intro.html] (Accessed 19 October 1997).

\textsuperscript{58} WIPO, “Issues relating to trademarks and Internet domain names”, \textit{above} n. 56.
These three TLDs are referred to as "generic" or "gTLDs". Anyone from any country in the world may register a SLD in a gTLD, thus they are also named "international" TLDs. Although people register freely in all three gTLDs, theoretically "org" is reserved for non-profit organisations, "com" for commercial entities, and "net" for networks.

(4) "int"

This TLD is reserved for international treaty organisations, such as the UN, WIPO etc. They must use their name or acronym as a SLD name, e.g. "www.wipo.int".

This paper will predominantly focus upon the TLD space "com".

2.2 The nature of a domain name

The domain name has a dual nature; it is both a name and an address. Hence it both identifies and locates Internet resources. In other words, they are similar to geographic names, which overlay a street address, postcode and country.59 Domain names have also been compared to the 1-800 telephone numbers that can be dialled as a mnemonic.60 Domain names serve as vanity telephone numbers for companies that want a number that is both easy to remember and guess. For example;

<table>
<thead>
<tr>
<th>numeric phone number</th>
<th>alpha-numeric phone number</th>
<th>numeric address</th>
<th>alpha-numeric domain name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-800-463-3339</td>
<td>1-800-GQFEDEX</td>
<td>192.83.161.5</td>
<td>fedex.com</td>
</tr>
</tbody>
</table>

59 Burk, above n. 2.
60 Burk, above n. 2.
As can be seen from the above, the DNS is quite similar to the numeric/alpha-numeric pairs for telephone numbers.\(^{61}\)

Moreover, each SLD name under the "\.com" suffix is unique; in other words, there is only one "xyz.com".\(^{62}\) Thus the grant of a registration has effect world-wide. Once "www.xyz.com" has been registered, it prevents use of that domain name by others anywhere in the world.

2.2.1 Are domain names property?

An interesting aspect of the nature of a domain name is the question of whether it is property. The answer to this question may have an impact upon what kind of transactions a domain name holder can perform and what kind of protection he or she will have against trademark owners. In the US, the Network Solutions, Inc.(NSI)\(^{63}\) has indicated in its policy that a domain name is property. In Network Solutions, Inc. v Clue Computing, Inc.\(^{64}\), NSI stated in a federal interpleader that it "has no interest in the property in dispute and is prepared to assign the registration and use of the "clue.com" domain name as determined by the court".\(^{65}\) The intellectual property lawyer

\(^{61}\) Frank, above n. 22.

\(^{62}\) Friedman, J.R., "Master your Internet domain name" (1997) 26 (1) The Magazine for Magazine Management 64 at 64.

\(^{63}\) For an explanation of the NSI and its role, see Chapter 1.3. above.


\(^{65}\) NSI filed an interpleader action against Clue and Hasbro pursuant to 28 U.S.C. paragraph 1335, claiming that it is an "impartial and unbiased stakeholder". The court granted the defendants' motion to dis-
Carl Oppedahl comments that “interpleader is available only with respect to property, and thus NSI had to take the position that the “clue.com” domain name was property”.66 However, if a domain name is property, how can US courts transfer domain names to the claimant as a remedy in trademark infringement cases? If a domain name may be said to be a trademark - that is, intellectual property - there is no precedence in traditional trademark law for transferring a trademark as a remedy for trademark infringement. On the other hand, the person or company that registers a domain name is called the “domain name holder”, not the “domain name owner”. In contrast, a person or company that has legal rights to a trademark, is called the “trademark owner”. One may ask whether this difference in terminology has any legal significance. If it means that a domain name is just a service, similar to the status of telephone numbers, then it is not property, and can more easily be transferred from one person to another.

miss. Judge Wiley Daniel wrote that: “[NSI] is not merely a disinterested stakeholder praying the Court to resolve a dispute between adverse parties. Instead, [it] is being sued [for] breach of contract...” “Current Developments” “NSI Cannot Interplead Domain Dispute, District Court Rules” (1996) 13 (12) The Computer Lawyer 29 at 29. According to Black’s Law Dictionary, an interpleader is “an equitable proceeding to determine the rights of rival claimants to property held by a third person having no interest therein. When two or more persons claim the same thing (or fund) of a third, and he, laying no claim to it himself, is ignorant which of them has a right to it, and fears he may be prejudiced by their proceeding against him to recover it, he may join such claimants as defendants and require them to interplead their claims so that he may not be exposed to double or multiple liability. A defendant exposed to similar liability may obtain such interpleader by way of cross-claim or counter-claim. Interpleader in federal court is governed by the Federal Interpleader Act, 28 U.S.C.A. paragraph 1335, and Fed. R. Civil P. 22”.

Oppedahl notes that NSI’s attempt to use federal interpleader in this case was ruled improper, however not because domain names are not property, but on other grounds. See Oppedahl’s footnote (17). Oppedahl, C., “Remedies in Domain Name Lawsuits: How is a domain name like a cow?”[WWW: http://www.patents.com/pubs/jmls.sht] (Accessed 22 August 1997).
In the US, people have transferred domain names to third persons, they have sold them, leased them and purchased them as if it was regular property. This practice illustrates that a domain name may be said to be property. Moreover, people have gone to court to attempt to obtain them. Does this practice mean that once NSI has granted a domain name, it is the holders’ to do whatever they want with it? According to RFC 1591 domain names are “delegated”. However, a RFC has no standing in a court of law. Critics have been complaining about NSI not following RCF 1591.

In contrast, in Australia the use of a domain name is by licence. Melbourne Information Technologies Australia (Melbourne IT), that is the administrator for the “com.au” domain name space, states in its policy that “Successful registration of a domain name results in a licence to use the domain name for a given period...The successful applicant is then referred to as the licensee of the domain name”. Hence there is a difference in terminology from that of NSI in the US. A licence is generally not regarded as property. Furthermore, the Melbourne IT policy states that “The domain name licence is non-transferrable”. Does this mean that if disputes occur, the Australian courts can not transfer the domain name as a remedy? As a solution, the Melbourne IT may revoke the domain name when disputed. The policy states that “The domain name licence may be revoked...where a court of competent authority determines that the domain name

67 Postel, J., “Domain Name System Structure and Delegation” [WWW ftp://ds.internic.net/rfc/rfc1591.txt] (Accessed 8 November 1997). Interestingly, the Nominet UK follows this terminology when it in its policy refers to the allocation of the domain name as “the delegation of the Domain Name”, see http://www.nic.uk/drs.html.

68 Steinberg, D., “Re: Are domain names sold or leased?” [Email “Domain-policy” mailing list] (Received 29 October 1997).

69 For an explanation of Melbourne IT and its role, visit http://www.melbourneit.com.au/

should not be allocated to the applicant, or should be allocated to another party”. In other words, Australian courts can rule that the domain name in question should be allocated to another party, and then the Melbourne IT will revoke the licence. However, when revoked, the domain name will “remain dormant for a period of three months”. After this period, the successful claimant in the court case can apply for the domain name afresh. A question may be raised whether this is a satisfactory solution for the successful claimant in a court case. In the US, the rationale behind the rapid transfers of domain names is that speed is crucial to the users of the Internet. On the Internet, everything happens fast and efficiently. This paper will argue that Australian courts are likely to transfer a domain name as a remedy in a lawsuit between a trademark owner and a “cybersquatter”. As precedence the courts may use the US cases, such as Intermatic, Inc. v Dennis Toeppen. Nevertheless, this has not been a significant problem in Australia until now.

However, one may argue that the question whether a domain name is property is not a question of whether the domain name has value or whether it can be bought and sold, but it is a question of whether the law chooses to protect the domain name from trespass. This question will not be further examined.

If the question whether domain names are property is answered in the affirmative, a related question is: Who owns them? Does the domain name registration authority own the domain names, in which case the domain name holder merely has a licence to use its domain name, as in Australia? Or is the party who has registered the domain

---

71 Melbourne IT, above n. 70.
72 Ibid
74 Eliseeva, M., “Is domain name property? Round 2” [Email - “Domain-Policy” mailing list] (Received 22 October 1997).
name, and who uses it, the legal owner of the domain name? Oppedahl suggests that the question may be merely one of semantics. This paper will defer this question and continue to refer to the entity who holds a registered domain name as the domain name holder.

2.3 The allocation of second-level domain names

As revealed above, until now, the " .com " TLD has been administered by the NSI. The NSI has allocated SLD names and provided the dispute resolution mechanisms when conflicts occurred. Therefore, it is important to examine the current NSI domain name allocation policy.

The latest edition of the policy, the fourth, became effective on September 9, 1996. Regarding the allocation of domain names, the most notorious principle in the policy is the "first come-first served" principle. This principle has been NSI's policy from the very beginning of the allocation of domain names under " .com " , and thus caused most of the issues regarding trademarks.

The relevant provisions state:

...second-level domain names [are registered] on a "first come-first served" basis....Network Solutions does not determine the legality of domain name registration, or otherwise evaluate whether that registration or use may infringe upon the rights of a third party...The Registrant...represents that...to the best of the Registrant's knowledge, [registration of the domain name] does not interfere with or infringe upon the rights of any third party...[and] that the Domain Name is not being registered for any unlawful purpose.

75 Oppedahl, "Remedies in Domain Name Lawsuits: How is a domain name like a cow?", above n. 66.

76 For a detailed and informative, however not objective, overview of the problems regarding the NSI policy, visit the "NSI Flawed Domain Name Policy information page" at http://www.patents.com/NSI.sht. The page is updated almost every month.


78 Ibid
In essence, the principle provides for an allocation of domain names on the basis that the first person or company that applies for the domain name will obtain it. Hence second-comers must settle for a different name. There is no examination as to whether the applicant is the most “legitimate” holder of the name, or whether there are other persons or companies that possess a better right to the name. The applicant must only sign a document stating that to his or her knowledge, the domain name does not interfere with the rights of third parties.

In comparison, Melbourne IT\textsuperscript{79}, the administrator for the third-level domain names under the “.com.au” domain name space, has a stricter policy. Firstly, only a legal entity which is a commercial entity that trades in Australia can register a “.com.au” domain name. Secondly, one commercial entity is allowed only one “.com.au” domain name.\textsuperscript{80} In contrast, the NSI has no such requirement. Consequently, the large moviehouses register a new second-level domain name for each new movie released; for example, “meninblack.com” and “hercules.com”. Thirdly, the domain name must be directly derived from the legal name of the commercial entity. Additional characters that do not appear in the full legal name of the commercial entity can not be used. The NSI has no such requirement. Finally, the applicant must ensure that the use of the domain name does not contravene any third party’s rights to the use of the name. In summary, even though the domain name allocation takes place on a first come-first served basis and there is no examination of the applicant’s and any third party’s rights, the Australian rules ensure that there is less likelihood of disputes and clashes. Moreover, if a dispute occurs the licence to use the domain name can be revoked until the dispute is settled. Nonetheless, in the future, there may occur domain name grabbing in Australia as well. As of 18 September,

\footnotesize
\textsuperscript{79} Visit http://www.melbourneit.com.au/

\textsuperscript{80} Melbourne IT, above n. 70.
1997, the well-known “Hungry Jack’s” had not yet been registered as “hungryjacks.com.au”.  

In Norway, the rules are similar to those of Australia. Uninett is the administrator of domain names under the country code “.no”. The registration is taken care of by NORID (The Norwegian Internet Domain Name Registry). Under the domain name policy, an applicant must represent or be a part of an organisation that is registered as such within Norway. Hence individuals may not register second-level domain names, but must register a third-level domain name under the domain name space “priv.no”. There is no counterpart to this provision in the NSI policy; for example, Dennis Toeppen managed to register more than 200 different domain names. Furthermore, NORID requires that the organisation “should be able to argue some degree of national significance”. This provision is thus stricter than the Australian counterpart. Similarly to the Melbourne IT policy, the organisation may register only one domain name. Moreover, the domain name must “refer in a reasonable way to the name of the organisation...either the full name, part of the name or a well-known abbreviation of the actual name of the organisation”.

---

81 A search for “www.hungryjacks.com.au” at http://www.aunic.net, on 18 September, 1997, resulted in no such domain name found. A new search was conducted on 8 November, however the result was: “This name is not visible to the DNS”.


83 Visit http://www.uninett.no/

84 Uninett, above n. 82.

85 Intermatic Incorporated v Dennis Toeppen, above n. 73.

86 Uninett, above n. 82.

87 Ibid
The Nominet UK administers domain names in the “.uk” TLD.\textsuperscript{88} The first come-first served rule for domain name allocation is maintained in the UK as well, as the Nominet states that “where two applications are for the same name then the one which is received first shall have prior claim”.\textsuperscript{89} It is worth noting that there is no limitation on the number of names that may be applied for.

In summary, the different national policies under the country code suffixes vary slightly. However, most of them are stricter than the NSI policy and seem to deal with the “domain name versus trademark” problem in a more efficient and satisfactory manner.

2.4 Background on the problems regarding SLD names under .com

Having defined domain names, considered the DNS and examined the current domain name allocation policies, this paper will now narrow its focus to the problems regarding the SLD names under the TLD “.com”. In the past couple of years, numerous national court cases have been filed by companies wanting to obtain a domain name or trying to stop someone else from using that domain name.

It is the SLD names under the TLD space “.com” that have raised most legal issues and discussions and caused the most problems in practice. Historically, the “.com” suffix was the domain name space for commercial entities in the US, omitting the country code “.us”. Now, several commercial entities all over the world have registered a SLD name under the “.com” space, and the number of registrations is increasing. As a consequence, the “.com” TLD name space became crowded. Hence disputes regarding SLD names under “.com”

\textsuperscript{88} On 1 August 1996 the company Nominet UK took over from the UK Naming Committee the responsibility for allocating UK domain names. Visit its homepage on http://www.nic.uk/

increased, mainly because at “.com”, in contrast to for example the “.edu” suffix, money is at stake. Thus, commercial entities prefer the “.com” TLD.

In principle, a domain name could be an arbitrary string of characters, no easier to remember than, for example, a street address. However, as a result of the user-friendly mnemonic address, companies want to register a SLD name that is easy to remember for their customers and potential customers. As mentioned above, it is important to obtain a SLD name that consists of the company’s trade name or acronym; that is, as close as possible to the company’s trademark. Ideally, companies want a name that is easy to deduce for their potential customers. Thus a logical address is important. However, there is a difference between the possibility of holding a name that is easy to remember and holding a name that is also easily guessed. In order to be easy to remember, first of all the domain name need to be short. Many television advertisements end with a WWW address which a viewer might use to obtain more information about the goods or services touted in the advertisement. However, a domain name easy to guess must be in close relation to the actual spelling of the trademark. Consequently, several weak trademarks, such as trademarks that consist of “International”, “National”, “Australian”, “Genesis”, “American”, “Acme” etc., will face problems when they decide to go online, since there is only one SLD name under the TLD “.com” to grant.90

The rationale behind the desire to possess a SLD name that is easy to guess lies in the function of a domain name. The domain name serves as an address, at which one can find the company or person holding the domain name. However, the domain name also serves as a directory. Users find their way through the WWW by guessing URLs. Hence a potential customer of, for example, IBM would expect to be able to find information about IBM products by typing

90 See Buerger, D.J., “Internet naming needs a face-lift to meet real-world needs” (1995) 12 (32) Network World 59 at 59. Buerger comments that cybermarketing on the Internet will depend on name recognition and today’s naming approach does not meet that goal. He states that if the Internet is lawless, it is inappropriate for business.
“http://www.ibm.com”. Furthermore, he or she might try “http://www.apple.com” and expect to find the competitor Apple Computers, in order to compare the products and prices. This illustrates the desire to obtain a logical and easily guessed domain name. However as the Internet grows and more entities register domain names, it may be impossible that domain names can remain “guessable”. Hence there will need to be an increased reliance on directory services and search engines.

2.5 Overview of the major problems regarding SLD names

To re-focus this thesis, it is important to note that when examining the domain name problems, there are three areas of issues that are significant:

* trademarks and domain names;
* trade and commerce aspects; and
* technical issues.91

This paper will focus on the conflicts between domain names and trademarks only.

The major problems regarding SLD names (note that hereinafter SLD names will be referred to as “domain names” unless otherwise expressly mentioned) under the TLD “.com” and trademarks have been:

* allocation of domain names,92

---

91 To my knowledge, the technical issues are not at stake. After subscribing to three different mailing lists on the domain name issue, my general impression is that the workload generated by the DNS will remain a very small fraction of the total traffic passing through the Internet. Hence the technical problems will always be solved, and thus form no obstacle to the further development of the Internet. See gTLD-MoU frequently asked questions [WWW - http://www.gtld-mou.org/docs/faq.html] (Accessed 20 August 1997).

92 See Chapter 2.3. above.
whether trademark law is applicable to Internet domain names and, if, whether a domain name infringes or dilutes a trademark;

- domain name grabbing. “Pirates” have intentionally registered famous trademarks as domain names and hoped that the companies will find it easier to pay them than to sue them. This is also referred to as “domain name hijacking”;

- one business legitimately holds a domain name after registering it with the NSI, but has no trademark rights in the name. Another business, with trademark rights in that name, desires to use it as its domain name. When the trademark owner then attempts to “grab the domain name back”, the situation is called “reverse domain name hijacking”;

- two or more businesses are inquiring the same domain name, and both/all of them have trademark rights in relation to the name or its acronym; and

- the dispute resolution policy. The NSI, after being faced with lawsuits from several trademark owners alleging trademark infringement, adopted a dispute resolution policy where the NSI suspends the domain name pending a dispute settlement.
Aims of chapter 3

The aims of Chapter 3 are to:

* provide an overview of trademark law in Australia, the UK and the US, relevant to the domain name issue; and

* examine some international agreements and treaties on trademarks to highlight the global trend towards harmonisation of the rules governing well-known trademarks.

Having outlined the domain name problems, it is important to have an understanding of the relevant trademark law. As mentioned above, Internet domain names are increasingly important in commerce. The WWW and its progeny are likely to be a major force in consumer retailing within a few years. Hence it is important for businesses to possess a domain name that links to its trade name. This chapter will examine trademark law in general, and more importantly the issues that arise due to the intersection between Internet domain names and trademarks.

3.1 Definition

A trademark is a brandname, and trademarks can be defined as words, symbols, or other devices used to distinguish the goods of one person from those of another.93 In section 17 of the Australian Trade Marks Act 1995 (C’wth) (hereinafter referred to as the “TM Act”), a trademark is defined as:

a sign used, or intended to be used, to distinguish goods or services dealt with or provided in the course of trade by a person from goods or services so dealt with or provided by any other person.94

---


The word “sign” in s. 17 of the TM Act is defined in s. 6. It includes the following or any combination of the following, namely, “any letter, word, name, signature, numeral, device, brand, heading, label, ticket, aspect of packaging, shape, colour, sound or scent”. Moreover, “word” in s 6 includes “an abbreviation of a word”.95

A servicemark is a trademark for services, such as “Qantas” for the airline. In this paper, “trademarks” will include servicemarks if not otherwise explicitly stated.

3.2 The rationale

The rationale behind a system of trademarks is to identify the source of goods. A trademark gives the consumer an indication of the source of origin.96 Thus trademarks provide product recognition in the national and international marketplace. Trademarks are important to merchants because they are means of attracting customers and accumulating consumer goodwill. The value of a trademark can be exceedingly high and has been described as a company’s most important and valuable asset.97 The trademark also ensures quality; the consumer can be sure that he or she gets the quality he or she expects. Moreover, the trademark enables the consumer to choose among competing products in a deliberate manner. The trademark system thus protects against confusion in the marketplace as a result of conflicting use of similar words or symbols.98

3.3 Examples

---


96 Rosenoer, above n. 1 at 95.


98 Rosenoer, above n. 1 at 95.
An example of a trademark being a word is the chocolate "Snickers", and an example of a phrase is “Don’t Leave Home Without It”. Moreover, trademarks can be pictures or symbols; for example, the window icon used by Microsoft, or numerals and letters, such as XXXX Gold. An example of a trademark which is an abbreviation, is IKEA, and an example of a nickname is Coke for Coca-Cola. A trademark can also be colours; for example, pink for Baskin 31 Robbins ice cream, or sounds and music, such as the Telstra advertising jingle.

3.4 The different types of trademarks

Trademarks can be categorised in five different categories: fanciful or coined trademarks, arbitrary trademarks, suggestive trademarks, descriptive trademarks and generic trademarks. Fanciful or coined trademarks are marks that are without any meaning at the time they are adapted (i.e. invented words). Examples are XXXX and Ajax. Arbitrary trademarks are marks that have a recognised meaning at the time one adopts them, but they do not relate to the product with which they are used. A classic example, is Apple for computers. Another example is Yahoo for an Internet search engine. Suggestive marks suggest a feature of the product; for example, Obsession for perfume. Descriptive marks merely describe a feature of the product. For example, Computerland for a computer store. Generic marks are words that are general or common names for the products to which they are applied. For example, beer for a type of alcoholic beverage.

3.5 Distinctiveness

Under Australian, UK and US law, distinctiveness is a key element for protection of a trademark. In Australia, s 17 of the TM Act, requires that the mark must be used or intended to be used, that there is a connection in the course of trade and that the mark is able to

---

99 American Express owns the famous trademark “Don’t Leave Home Without It”.
100 Smedinghoff, above n. 93 at 212.
distinguish the good from other goods. This paper will deal with the latter requirement only.

As the distinctiveness requirement in the UK, US and Australia is similar, this paper will examine the requirement in the TM Act s 17 only. Section 17 requires goods or services to be distinguished. The distinctiveness requirement is also called the strength of a trade-mark.\(^{101}\) As a result of this requirement, even if a mark falls within the definition of trademark, it will not necessarily be registrable.\(^{102}\) The rationale behind this requirement is that since the registration provides the trademark owner with a monopoly, there is a reluctance to grant such exclusive rights for a word that is commonly used in the English language.

Fanciful marks as XXXX are very strong marks because they have no recognised meaning. Consequently, the consumers assume they are indications of source rather than description of products. Arbitrary marks such as Apple are also strong, because they have no meaning in the context in which they are applied. In contrast, suggestive and descriptive marks are weaker because they refer to the quality or function of the product. Thus they are not good indicators of origin. A descriptive mark is not distinctive and thus it does not qualify as a trademark until it has gained public recognition as one. This recognition is called acquired distinctiveness or secondary meaning. One example of secondary meaning is Calvin Klein. Similarly, generic terms can not be registered as trademarks. They describe what the product is rather than give an indication of source, such as "milk". Hence generic terms do not distinguish between different brands and do not fulfil the distinctiveness requirement.

In the US, there is a concept of inherent distinctiveness. Fanciful, coined and arbitrary marks are regarded as inherently distinctive.\(^{103}\)

\(^{101}\) Ibid


Descriptive names, on the other hand, may become distinctive, and after five years there is a presumption of distinctiveness. In contrast, there is no such presumption in Australia.

The chart below depicts the ascending order of distinctiveness and strength of protection of a trademark:\[104\]

<table>
<thead>
<tr>
<th>Protectable</th>
<th>No protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbitrary</td>
<td>Descriptive</td>
</tr>
<tr>
<td>Generic</td>
<td>Ge-</td>
</tr>
<tr>
<td>Fanciful</td>
<td></td>
</tr>
<tr>
<td>Coined</td>
<td></td>
</tr>
</tbody>
</table>

---

3.6 Acquisition of trademark rights

3.6.1 Actual use and registration

The trademark must be used or registered as a trademark in order to acquire trademark protection. The protection can be obtained through common law or statute law. At common law, the way to acquire ownership in a trademark is to use it and acquire reputation in it. In Australia, the proprietorship arises from "the combined effect of authorship of the mark, the intention to use it upon or in connection with the goods and the applying for registration". Hence in Australia a trademark can exist both by common law or by registration. In contrast, some civil law countries do not recognise common law trademark rights. Instead, they follow a strict registration concept, where the first party to register the mark receives exclusive rights to that mark. Thus unregistered marks receive no legally recognised protection. However, it is beneficial to register the trademark in common law countries, because then there will be a presumption of distinctiveness. Section 41 (2) of the Australian TM Act requires that a trademark application be rejected if the trademark is not capable of distinguishing the applicant’s goods or services from those of other persons. Without this presumption, the burden of

105 In Australia, s 20 (1) of the TM Act provides that registration gives the registered owner an exclusive right to use the trademark and to obtain relief for infringement. As mentioned, the registration also provides the trademark with a presumption of distinctiveness.

106 McKeough and Stewart, above n. 102 at 427.

107 Shell Co of Australia Ltd. v. Rohm & Haas Co (1949) 78 CLR 601 at 625. See also McKeough and Stewart, above n. 102 at 427.


109 Trade Marks Act 1995 s 41 [WWW -http://www.austlii.edu.au/au/legis/cth/num_act/tma1995121/s41.html] (Accessed 27 August 1997). Registration of the trademark takes effect from the date of application (s 72 (1)). Registration subsists for seven years (s 72 (3)) and
proof will be heavier. Another advantage of registration is that the trademark will obtain an Australia wide market.

Similarly, in the US, there is no need for registration of the trademark. A person acquires trademark rights by using a trademark in commerce to distinguish goods or services from those of others. However, trademarks may be registered with federal or state authorities. In addition, registration may be filed prior to actual use, under the “intent-to-use” provision of the Lanham Act, paragraph 1051 (b). Registration provides jurisdiction in federal courts for infringement claims without the necessity of demonstrating diversity of citizenship. Likewise, the Lanham Act provides the possibility of receiving treble damages and attorney fees upon proving infringement. These generally are not available under the common law. Another benefit of registration is the presumption that the registrant is the owner of a valid trademark. Further, after five years of registration may be renewed thereafter for an indefinite number of further periods of ten years (s 77 (1)). McKeough and Stewart, above n. 102 at 431.

110 Smedinghoff, above n. 93 at 214.

111 Smedinghoff, above n. 93 at 215.

112 The US Lanham Act, above n. 103. In the US, the first person who uses the trademark has priority over others who use it. In other words, the period of priority starts when one start to use the mark. In a conflict, the party having priority prevails. In Australia, registration takes effect from the date of application, s. 72 (1). However, the registration of a trademark relates to a particular class of goods (e.g. cars and foodstuff are two different classes) and a particular market (e.g. Australia is one market). Thus priority is measured with respect to that particular geographic territory, market or channel of trade, and hence two persons can have priority with respect to the same trademark in two different markets. Moreover, the same or similar trademarks can exist for different classes of goods within the same market; for example, Festivia car and Festivia pasta. This may cause problems in cyberspace. The Internet transcends geographic territories, different markets and different classes of goods, thus there may be a conflict if both Festivia cars and Festivia pasta want to go online. This is a consequence of the fact that within the most popular top-level domain name, “.com”, there is only one second-level domain name to grant. This issue will be examined further in Chapter 4.
certain challenges or defences to the trademark are precluded altogether. Finally, and perhaps the most important benefit, registration allows the trademark owner to acquire rights in the trademark in a greater geographical area than often would be possible under common law.

3.6.2 What kind of use is required to acquire trademark protection?

As mentioned above, one can obtain reputation in a trademark through use of the trademark in the marketplace. In practice, this requirement is fulfilled by labelling one’s goods. However, one must distinguish between tangible goods and digital goods. With respect to tangible goods, one is required to physically place the mark directly onto the goods or their packaging.113 Digital goods (e.g. software distributed online) can not be marked physically. However, it should be possible to obtain trademark protection for these kinds of goods as well. For example, one can use the trademark as the name of the files containing the digital goods and present the trademark to users at the time they purchase the goods. Furthermore, a service-mark may be used by appearing on the web site as a logo.

3.6.3 Registration of domain names as trademarks

A complex question of use is whether an Internet domain name can be registered as a trademark. For example, an online magazine can name its page on the Internet “cybermagazine.com”. The question is whether this domain name can qualify as a trademark. In order to qualify as a trademark, the domain name should fulfil the requirements of distinctiveness as examined below.

In the UK, the UK Trade Marks Registry has issued a statement concerning “Registration of Internet Domain Names as Trade Marks”.114 The Registry’s statement explains its current practice concerning applications to register trademarks comprising what ap-

---

113 Smedinghoff, above n. 93 at 214.

114 See the UK Trade Mark Registry, “Registration of Internet Domain Names as Trade Marks” March 12, 1997 (6166) U.K. Trade Marks Journal.
pear to be domain names. The UK Registry’s view is that the generic part of the domain name, such as “.com”, is “non distinctive and should be regarded as devoid of any distinctive character as a trademark for goods or services put on the market via the Internet”.

In the US, the US Patent and Trademark Office (PTO) has issued a policy for handling this new breed of mark. The PTO distinguishes between content, service and link providers. Similarly to the policy in the UK, the PTO states that the prefix (i.e. “http://www.”) and the suffix (i.e. “.com”) of the URL are not given weight in the analysis.

As a result of the Internet being a digital medium, a practical limitation is that there can be no sounds, scents, picture symbols or similar non-alpha numeric symbols used as a domain name.

### 3.7 International trademark filing agreements

Because various sovereign nations provide for trademark protection on a national basis, generally a trademark registration protects the mark in only that one country. Hence registration with foreign authorities will expand the trademark rights. If a trademark owner desires protection in multiple countries, separate applications must be filed in each country where he or she intends to use the mark.

Filing applications in multiple countries is often complicated, time consuming and expensive. In order to simplify the process, some

---


116 Morton, above n. 115.


119 Halpern, above n. 108.
countries are members of international trademark filing agreements.\textsuperscript{120}

It is interesting to note that when a trademark owner has developed a reputation in one market, for example Australia, and then goes online to sell the product on the Internet, the application of the trademark extends its market. Consequently, the mark may acquire common law trademark rights in new markets. The mark is then used as a trademark in a new market and may be said to comply with the common law requirement of usage and acquisition of reputation in a market. However, as a result of the global nature of the Internet there are several countries with access to the Internet that do not recognise common law trademark protection. The solution may be to have the trademark registration expanded to the markets the trademark is now trading in. This issue is not within the ambit of this paper.

### 3.8 Trademark infringement and dilution

In summary, a trademark can serve many functions, including: (1) distinguishing between the goods and services of one person and those of others; (2) identifying the source of origin of goods and

\textsuperscript{120} The \textit{Madrid Agreement Concerning the International Registration of Marks of April 14, 1891} is an example of an international filing agreement. If a country is a member of the \textit{Madrid Agreement}, a trademark is first registered in the home country. This application is then used as the basis for an international registration. [WWW - http://www.wipo.org/eng/iplex/wo_maa0_.htm] (Accessed 13 November 1997). See also the \textit{Madrid Protocol, June 28, 1989, and Common Regulations under the Madrid Agreement Concerning the International Registration of Marks and the Protocol Relating to that Agreement, and schedule of fees} (April 1, 1996) at the same site as the \textit{Madrid Agreement}. Similarly, EU has a system of Community Trade Marks, co-existing with each EU nations' own trademark system. Through the filing of a single application, a Community Trade Mark provides registration in all EU countries. Community Trade Marks are available to non-members of the EU, as long as the trademark owner has a commercial establishment in a country which is a member of the \textit{Paris Convention for the Protection of Industrial Property}. Thus, Australian trademark owners may apply for a Community Trade Mark.
services; (3) preventing consumer confusion; (4) assisting consumers in identify and re-identify goods and services of a particular producer; (5) guaranteeing the quality or other characteristics of the goods or services; (6) protecting the goods from passing off; and (7) advertising the goods or services. These functions of a trademark illustrate the importance of protecting trademarks from infringement and dilution.121

3.8.1 Australia

The TM Act s 120 outlines when a registered trademark is infringed.122 Firstly, subsection (1) states that a registered trademark is infringed if someone uses a sign that is “substantially identical with, or deceptively similar to” the trademark in the same class of registration. In other words, the goods in question must operate in the same class of goods in order to constitute an infringement.

Secondly, subsection (2) states that use of a substantially identical or deceptively similar sign as a trademark, in services “closely related to” the registered goods, or in services or with goods of the “same description” as that of the registered goods, also constitutes infringement. In addition, section 120 (2) requires that there is a likelihood of confusion. The requirement is a consequence of the fact that the products are in different registration classes, and only operate in the same market. When the trademarks are registered in different classes they are less likely to confuse the consumers. Generally, consumers are used to seeing the same trademark in the same market on different types of products, without confusing the products. In other words, when operating in different classes of goods it is a defence

121 See Chapter 4 regarding use of trademark law on conflicts between trademarks and second-level domain names.
against the infringement allegation that there is no likelihood of confusion or mistake.\textsuperscript{123}

Thirdly, section 120 (3) deals with so-called well-known trademarks.\textsuperscript{124} It states that infringement may occur where the trademark in question is “well-known in Australia” and the sign used is “substantially identical with, or deceptively similar to” the well-known trademark, regardless of a relationship between the goods or services. Hence there is no requirement of likelihood of confusion in s 120 (3). This may be partly explained by subsection (3) (b), which states that since the trademark is well-known, it is deemed likely to be connected to the sign allegedly infringing it. In subsection (3) (d) there is a presumption that this connection is unfavourable for the trademark owner. Thus there is a general likelihood of confusion, and the owner of a famous trademark need not prove any specific likelihood. In effect, s 120 (3) brings a new dimension to Australian trademark law - the concept of infringement by association.\textsuperscript{125} To date there have not been any cases decided in which s 120 (3) is at issue. However, the courts will probably look for a likelihood of confusion as a result of the requirement “would be likely to be taken as indicating a connection”. When courts decide whether the mark is a famous trademark according to subsection (4), the extent to which the trademark is known in the relevant sector of the public, regardless of how the mark became famous, must be taken into account.\textsuperscript{126}

\textsuperscript{123} McKeough and Stewart, \textit{above n. 102} at 458

\textsuperscript{124} Section 120 (3) implements Article 16 (2) and (3) of the TRIPS Agreement.

\textsuperscript{125} Evans, G., “The Impact of Public Legislating under the Trade Constitution on Municipal Law: A Case Study of Australian Trade Mark Legislation” (chapter six of an unpublished paper). Gail Evans purports that so far the owners of well-known trademarks do not have to prove confusion, the impact of s 120 (3) is considerable. The subsection offers protection in those cases where the public may possibly associate the product in question with the trademark, and for that reason adversely affect the owner’s interests.

\textsuperscript{126} In comparison, see the US \textit{Federal Trademark Dilution Act of 1995} (implemented in the \textit{Lanham Act} s 43 (c), i.e. U.S.C. Title 15 Chapter
How can this impact on a situation where an owner of a well-known trademark discovers that his/her registered trademark is used by someone else as a domain name? How can he or she obtain the domain name? Chapter 4 will focus upon these issues.

3.8.2 The United States

In the US, one can allege trademark infringement on a similar basis to the Australian likelihood of confusion requirement. In addition, one can allege dilution. Since the US notion of likelihood of confusion is similar to that of Australia, this section will focus on the notion of dilution. In the US Federal Trademark Dilution Act of 1995 (US Dilution Act), section 3 (c) (1) states that the owner of a famous trademark is entitled to an injunction against another person's "commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark". Australian law does not have an equivalent section, however one may argue that s 120 (3) of the TM Act; or perhaps passing off, and misleading or deceptive conduct actions based on s 52 of the Trade Practices Act 1974 (C'th), may give similar protection.

The term "dilution" is defined in the US Dilution Act s 4 as:

the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of:

(1) competition between the owner of the famous mark and other parties; or

---


127 See the US Lanham Act, above n. 103.


Consequently, there is no need for the owner of a famous trademark to prove that there is any likelihood of confusion. This is very similar to the *Australian TM Act* s. 120 (3). Moreover, the owner of the famous trademark and the infringer need not operate in the same class of goods or the same market. However, the infringing use of the trademark must cause dilution, that is “lessen the capacity to identify and distinguish” the products. A possible interpretation, is that the likelihood of confusion requirement comes in the backdoor. Prior to the *US Federal Dilution Act*, there were 25 different US state dilution statutes. Under these statutes, the courts dismissed dilution claims unless there was also a finding of infringement based upon a likelihood of confusion. On the other hand, based upon a literal interpretation of the Act, there need not be any likelihood of confusion for dilution to occur. “Dilution” is a requirement different from and not as onerous as “likelihood of confusion”. The *US Dilution Act* only requires that the trademark is famous and is used in commerce by one other than its owner for dilution to occur.

---

130 See the US *Lanham Act*, above n. 103.
131 The *Lanham Act* paragraph 1125 (c), above n. 126.
134 When the courts decide whether a mark is famous, section 3 (c) (1) requires that they take into account certain factors. However, the list of factors is neither exhaustive nor binding; “a court may consider factors such as, but not limited to—”. In comparison, see the list of factors in the *Australian TM Act* s 120 (4), above n. 94. Also see the international agreements protecting well-known trademarks, Chapter 3.9. below.
the different state dilution laws, the courts developed the notion of “blurring” or “tamishment”. 135 “Blurring” is typically the whittling away of distinctiveness caused by the unauthorised use of a trademark on dissimilar products, while “tamishment” refers to unauthorised use of a trademark which links it to products that are of poorer quality. 136 The legislative history cites as examples of uses which would fall within the US Dilution Act, the trademark BUICK for aspirin and KODAK for pianos.

The sign allegedly infringing the famous trademark must be used “in commerce”. This means that use of the famous trademark outside of trade will not be actionable. Section 3 (a) (4) (B) explicitly exempts non-commercial use. The “in commerce” requirement will be examined in Chapter 4. One may raise the question whether the use of a famous trademark as an Internet domain name causes dilution of the trademark. This issue and the issue of defences against allegations of dilution will be addressed in Chapter 4.137

3.8.3 The United Kingdom

The situation in the UK is similar to that of Australia. The UK Trade Marks Act of 1994 requires, in section 10 (2), that the plaintiff shows there exists a “likelihood of confusion on the part of the public”.138 Subsequently, s 10 (6) requires the court to consider whether

---

135 Ladas & Parry, above n. 132.
136 Ibid
138 The UK Trade Marks Act of 1994. According to s 10 (2), the defendant infringes if there “exists likelihood of confusion on the part of the
the particular use complained of "without due cause takes unfair advantage of, or is detrimental to, the distinctive character or repute of the trade mark".\textsuperscript{139}

3.9 International harmonisation of the protection of well-known trademarks

As seen above, trademarks are a national concern.\textsuperscript{140} However, globalisation and rapid technological change are changing the boundaries of intellectual property rights. There is no international registration of trademarks, however there is an international trend towards harmonisation. The essence of the concept of harmonisation is that national, state and society boundaries are permeable, and thus there is a sharing of legal principles among nations resulting in the creation of an international or extra-national value system.\textsuperscript{141} It must be asked whether there is a need for harmonisation of national and regional laws concerning trademarks and domain names. As a result of the worldwide scope of the Internet, intellectual property issues have obtained a new dimension.\textsuperscript{142}

\textsuperscript{139} The \textit{UK Trade Marks Act of 1994}.

\textsuperscript{140} \textit{The Paris Convention for the Protection of Industrial Property} March 20, 1883. Last amended in 1979. [WWW - http://www.wipo.org/eng/iplex/wo_par0.htm] (Accessed 6 November 1997). Article 6 (1) states: "The conditions for the filing and registration of trademarks shall be determined in each country of the Union by its domestic legislation". Hence it is clear from this convention that trademarks are a national concern and no agreement for the establishment of international marks has yet been achieved.

\textsuperscript{141} Kenna, \textit{above n. 97} at 47.

\textsuperscript{142} WIPO, "Possible issues to be considered in the context of harmonisation of national and regional laws concerning trademarks and Internet domain names" [WWW -http://www.wipo.org/eng/Internet/domains/tdn/cm/cm_ii_2.htm#note1] (Accessed 22 July 1997). See Chapter 6.1. below.
As an illustration of the ongoing process of international harmonisation of intellectual property rights, this chapter will examine some of the current treaties protecting well-known trademarks. In Chapter 4 there will be a discussion on whether we need a new international intellectual property concept, so-called cybermarks, to cope with the new challenges.

3.9.1 The Paris Convention

There are several international treaties to protect well-known trademarks. However, the different global, regional and bilateral treaties provide different standards of protection. In addition, the phrases “famous trademark” and “trademark well-known in...” have been interpreted differently. A mark defined as “well-known” is known to a substantial segment of the relevant public, whereas a "famous" mark has been defined as one that is known to a large section of the public. The rationale is thus that famous trademarks have a higher degree of reputation than well-known trademarks, and therefore deserve broader protection, that is, protection against use on non-competing goods and services.

The Paris Convention for the Protection of Industrial Property Article 6bis states

(1) The countries of the Union undertake, ex officio if their legislation so permits, or at the request of an interested party, to refuse or to cancel the registration, and to prohibit the use, of a trademark which constitutes a reproduction, an imitation, or a translation, liable to create confusion, of a mark considered by the competent authority of the country of registration or use to be well-known in that country as being already the mark of a person entitled to the benefits of this Convention and used for identical or similar goods. These provisions shall also apply when the essential

---


part of the mark constitutes a reproduction of any such well-known mark or an imitation liable to create confusion therewith....

(3) No time limit shall be fixed for requesting the cancellation or the prohibition of the use of the marks registered or used in bad faith.\(^{145}\)

*The Paris Convention* was the first international treaty to pronounce that well-known trademarks are protectable property.\(^{146}\) The Convention protects a trademark that is “well-known in that country”. Moreover, a “competent authority of the country” must determine whether a trademark satisfies the criterion. In other words, it is up to each country to govern this issue. Furthermore, the Convention does not define the relevant audience which must know the mark, nor how much of the audience must know the mark. In Germany, for example, knowledge must exist among over 50% of the audience to establish “notoriety”.\(^{147}\) As seen above, Australian law requires that the trademark is “well-known in Australia”,\(^{148}\) whereas the *US federal dilution Act* requires that the trademark is “famous”.\(^{149}\) Conse-

\(^{145}\) *The Paris Convention for the Protection of Industrial Property, above n. 140*. The convention is not self-executing, i.e. each country must implement the treaty through its own legislation.

\(^{146}\) *Squyres, above n. 143*.

\(^{147}\) *Ibid*

\(^{148}\) *Trade Marks Act s 120, above n. 94*. Note that section 120 (3) was implemented to conform with the TRIPS Agreement. Prior to the TRIPS, there was no additional protection of well-known trademarks in Australia. An unpublished paper by Gail Evans, *above n. 125*, points out that “Prior to the TRIPS Agreement of 1994, the impact of international law on Australian trade mark legislation was limited. The implementation of the trade mark provisions of the Paris Convention had been gradual and in some instances, most notably that of well known marks, entirely neglected...although Australia has been an independent contracting country to the Paris Convention since 1925, the government had been under no compulsion to comply with the undertaking in Article 6bis regarding protection of well-known trade marks until the TRIPS Agreement affirmed and extended their protection”.

\(^{149}\) *The US Dilution Act, above n. 126*. In other words, there might be more difficult to obtain the additional protection in the US than for example in Australia.
consequently, these different national standards will provide different standards of protection.

The Convention does not require that the trademark must be used in a country to be considered well-known therein. However, most countries have made “use” a requirement for protection. For example, in common law countries, protection of well-known trademarks developed from the “passing off” action.150 “Passing off” is an attempt by traders to pass off their goods as those of another. Five characteristics, indicated by Lord Diplock in the *Advocaat* case,151 are said to be required of a successful action.

Finally, it should be noted that the *Paris Convention* requires that there is confusion. In other words, the Convention is not an international dilution statute.

### 3.9.2 TRIPS

Another treaty that provides far greater protection of well-known trademarks is the *Agreement on Trade Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods of the General Agreement on Tariffs and Trade* (TRIPS).152 TRIPS is one

150 McKeough and Stewart, *above n. 102* at 356.

151 *Erven Warnink v. J Townsend & Sons (Hull) Ltd* [1979] AC 731 at 742. The five characteristics are: (1) a misinterpretation; (2) made by a trader in the course of trade; (3) to prospective customers of his [sic] or ultimate consumers of his goods or services supplied by him; (4) which is calculated to injure the business or goodwill of another trader (in the sense that this is a foreseeable consequence); and (5) which causes actual damage to a business or goodwill of the trader by whom the action is brought or (in a *quia timet* action) will probably do so. In other words, in a “passing off” action, a mark is protected only if it has reputation within the country. Usually, a reputation is gained through use. However, in the McDonald’s case in South Africa it was held that a mark can be well-known merely through reputation, without use in the jurisdiction. In the Australian TM Act s 120 (4), the trademark may be well-known as a result of promotion or any other reason. McKeough and Stewart, *above n. 102* at 356.

152 *TRIPS* was signed by the Members of GATT on 15 April 1994 at Marrakesh, Morocco. View *TRIPS* at [http://www.uspto.gov/web/offices/](http://www.uspto.gov/web/offices/).
of the international agreements of the Uruguay Round concluded in 1994 of the World Trade Organisation (WTO), the successor of the General Agreement on Tariffs and Trade (GATT). Two of the articles of TRIPS that are important in the trademark context state:

Article 16(2): “Article 6bis of the Paris Convention (1967) shall apply, mutatis mutandis, to services. In determining whether a trademark is well-known, account shall be taken in the relevant sector of the public, including knowledge that a Member obtained as a result of the promotion of the trademark”.

Article 16(3): “Article 6bis of the Paris Convention (1967) shall apply, mutatis mutandis, to goods or services which are not similar to those in respect of which a trademark is registered, provided that use of that trademark in relation to those goods or services would indicate a connection between those goods or service and

the owner of the registered trademark and provided that the interest of the owner of the registered trademark is likely to be damaged by such use”.

As can be seen from article 16, well-known trademarks are given a higher standard of protection than the majority of trademarks not so differentiated. Moreover, article 16 (2) recognises that harm can re-
suit from either actual use or promotion. Article 16 (3) provides that use which would indicate a connection between the goods or services of the owner of the well-known trademark and the dissimilar goods or services of another person would be forbidden if the interests of the owner of the well-known mark is likely to be damaged by such use. This standard is based on an association in the mind of the relevant public between the goods and the trademark in question.\textsuperscript{154} However, the mark must be registered in order to receive protection against use on dissimilar goods. The provision is implemented in the Australian TM Act s 120 (3).\textsuperscript{155}

In summary, well-known trademarks are protected by many treaties. There is a clear international trend towards harmonisation of the rules governing well-known trademarks; moreover, this trend points to increased protection.\textsuperscript{156} How will this impact on the disputes be-

\textsuperscript{154} Squyres, \textit{above n. 143} at 3.

\textsuperscript{155} See McKeough and Stewart, \textit{above n. 102} at 430. The Trademark Law Treaty 1994 (TLT) is also worth mentioning. It harmonises procedural aspects of trademark law. A provision that was omitted from the current TLT, but that may be said to indicate a global trend towards enhanced protection of well-known and famous trademarks, is article 103 (2) [WWW - http://www.wipo.org/eng/iplex/wo_tlt0.htm] (Accessed 14 November 1997). See also the NAFTA (\textit{North American Free Trade Agreement}) article 1708 (6) which refers to the \textit{Paris Convention} article 6bis. It is noteworthy that NAFTA declares that a party can never be required to prove that the reputation of its trademark extends beyond the relevant sector for the product or service. This is thus a narrowing of the relevant audience. [WWW - http://the-tech.mit.edu/Bulletins/nafta.html] (Accessed 13 November 1997).

\textsuperscript{156} Europe began its harmonisation process through the European Union (the EU), formerly the European Economic Community (EEC). In 1989, the EU harmonised the different trademark laws of the member states through the \textit{European Harmonisation Directive}. In articles 4 (3) and 4 (4), the Directive states that the owner of trademarks with "reputation" in the EU can stop the registration of a similar mark. This is also the case for the use of a mark on dissimilar goods or services (article 5 (2)). However, it is interesting to note that the EU, consisting of mostly civil law countries, uses the concept of reputation. As mentioned, this concept was developed in common law countries through the use of the "passing off" action. The \textit{European Harmonisation Di-
tween a well-known trademark and a registered domain name? Will this strong protection of famous trademarks lead to an increase in “reverse domain name hijacking”? 

rective formed the basis of several provisions of the Community Trade Mark Regulation (CTMR), adopted in 1994. Squyres, above n. 143. See the relevant CTMR articles 8 (1) (a) and (b), 8 (2) (c), 8 (5) and 9 (1) (c). The CTMR goes further than the Directive in terms of protection of famous trademarks. Under the CTMR, “likelihood of association” can be used as a basis for opposing the registration of a CTM, section 8 (1) b). It seems like the “likelihood of association” is a broader standard than the “likelihood of confusion” standard.
4 THE INTERSECTION BETWEEN TRADEMARKS AND SECOND-LEVEL INTERNET DOMAIN NAMES

As the dimensions of the tree are not always regulated by the size of the seed, so the consequences of things are not always proportionate to the apparent magnitude of those events that have produced them

- Charles Caleb Colton

Having provided an overview of trademarks and domain names, the aim of Chapter 4 is to bring the two issues together. When dealing with the inconsistencies between domain names and trademarks, trademark law has been utilised. Chapter 4 will analyse whether trademark law is applicable to domain name conflicts. Then the proposal of a cybermark will be examined.

Aims of chapter 4

The aims of Chapter 4 are to:

* critically analyse how domain names and trademarks collide, why they clash, and examples of conflicts in court cases and out-of-court settlements
* analyse whether contemporary trademark law can provide the mechanisms for effective regulation of domain name issues
* examine one possible solution - the proposal of a cybermark.157

157 See Chapter 4.7. below.
4.1 The intersection between trademarks and domain names

4.1.1 The differences and similarities between trademarks and domain names

As stated in Chapter 2, the SLD names under the TLD space " .com " are usually named after the company's trade name or an acronym thereof. The domain name can tell a person where on the Internet s/he has been, where he or she is now, who he or she is dealing with and how he or she can find them again. Thus the domain name may create an expectation about the nature of a product or the identity of a person or organisation. In other words, trademarks and domain names may serve the same function.158

However, the disharmony between domain names and trademarks also occurs as a result of the differences between them. As seen in Chapter 3, traditional trademark law allows identical registrations of the same trademark for non-competing goods or services, provided that there is no likelihood of confusion. Hence Domino Pizza and Domino Sugar may co-exist in real space. In cyberspace, under the same TLD space, the SLD domain names must be unique, thus there can be only one "domino.com". Moreover, another difference that may be a source of conflict is the fact that a SLD domain name can be generic, whereas trademarks must be distinctive. On the Internet “milk” and “cereal” can be registered as domain names.159


159 For example, the NSI has registered 200 domain names for Procter & Gamble Co., including “badbreath.com”, “dandruff.com” and “diarrhea.com”, and 150 domain names for Kraft General Foods Corp., such as “saladdressing.com” and “frozendinners.com”. Messmer, E., “Internet domain names free no more” (1995) 12 (38) Network World 8 at 8.
These differences and similarities can result in conflicts between domain name holders under “.com” and trademark owners. Owners of weak trademarks (i.e. suggestive and descriptive trademarks)\textsuperscript{160} are likely to collide when they attempt to obtain a domain name under the global domain space “.com”. This chapter will examine conflicts between SLD names under the TLD space “.com” and owners of trademark rights.

4.1.2 The different scenarios of possible conflicts

The legal issue that arises out of the conflicts described above is whether trademark law is applicable to the disputes between SLD names and trademarks. It is important to distinguish between the different scenarios that may occur.

1) Domain name grabbing. This is typically a conflict between an owner of a strong trademark (e.g. a well-known trademark, such as “Ansett Australia”) and a person that has registered the domain name on the first come first served basis (e.g. “ansettaustralia.com”) with the intention to obtain a “ransom” from the owner of the trademark. The domain name hijacker has often registered several famous trademarks as domain names, and is willing to transfer the domain name for money, hoping that the trademark owner will find it easier to pay than to sue the person. See for example, the \textit{Intermatic, Panavision, Kaplan} and \textit{McDonalds} cases.\textsuperscript{161}

2) The conflict between two or more owners of weaker trademarks that both or all desire the same domain name under “.com”; for example, \textit{the Prince case} and \textit{the Roadrunner case}.\textsuperscript{162}

3) The conflict between an owner of a trademark and a domain name holder without trademark rights to the domain name. The domain name holder registers the domain name first, under the first

\textsuperscript{160} See Chapter 3.5.

\textsuperscript{161} This was the case when Dennis Toeppen registered more than 200 domain names. See \textit{the Intermatic case, above n. 73}, examined in Chapter 4.2.3. below.

\textsuperscript{162} See Chapter 4.2.4 and 4.5. below.
come-first served principle, with the intention to use it as his or her legitimate domain name. Later on, the owner of the trademark wants the same domain name when he or she goes online. This “domain name envy” may result in reverse domain name hijacking where the trademark owner alleges trademark infringement or dilution to obtain the domain name he or she desires.

4) The conflict between two domain name holders with confusingly similar domain names. The emergence of cybermarks (i.e. domain name that have obtained reputation entirely through Internet presence) has lead to this type of conflict; for example, the conflict between Women’s Wire and Wired Magazine.163

<table>
<thead>
<tr>
<th>Possible conflicts:</th>
<th>trademark owner</th>
<th>domain name holder</th>
</tr>
</thead>
<tbody>
<tr>
<td>trademark owner</td>
<td>2) tm and tm</td>
<td>3) dn and tm</td>
</tr>
<tr>
<td>domain name holder</td>
<td>1) tm and dn</td>
<td>4) dn and dn</td>
</tr>
</tbody>
</table>

163 Burk, above n. 2. The conflict between Women’s Wire and Wired Magazine is examined in Chapter 4.2.5 below.
4.1.3 Is trademark law applicable to domain name conflicts?¹⁶⁴

Having outlined the different scenarios, this section will examine whether contemporary trademark law provides the mechanisms for regulation of domain name issues.

In several cases in the US, when dealing with the conflicts described above, the courts have utilised traditional trademark principles. Thus the courts have, without question, assumed that trademark law is applicable.¹⁶⁵ The NSI policy also links domain names to trademarks and trademark law. This link is criticised as artificial.¹⁶⁶

The concept of likelihood of confusion and the notion of dilution does not fit well with the domain name disputes. Also, there is a question whether the trademark owner should be allowed to allege trademark infringement or dilution when a corporate decision to go online is belated, the company discovers that the domain name it wants is taken, and the holder of the domain name possesses a le-

¹⁶⁴ Note that in Australia, The Corporations Act 1989 (C’wth) [WWW - http://www.austlii.edu.au/au/legis/cth/num_act/ca1989172/s343.html] (Accessed 9 November 1997), requires in s 343 that a foreign company “shall not establish a place of business, or commence to carry on business, within the Territory unless it is registered under this Division”. As a consequence, Australia is the only country in the world where the hamburger restaurant “Burger King” is called “Hungry Jack’s”. Burger King, when entering the Australian market, had to register another name because their trade name was already taken. The Act may have significance within the domain name versus trademark context. However, this paper chooses not to examine the issue.

¹⁶⁵ For example, in the Playboy Enters v Frena case, the court assumed without discussion that the trademark law applied (839 F.Supp 1552, 1559-61 (MD Fla 1993)). Brunel A., “Trademark Protection for Internet Domain Names” (1996) 24 (4) International Business Lawyer 174 at 177. In Australia, the disputes may involve trademark infringement, TM Act s 120, there is also the possibility of infringement of s 52 of the Trade Practices Act and for actions in passing off. See Fair, P. and Delabaere, N., “Your clients on the Internet. Some practical law on domain names and trade marks” (1995) (12) Law Society Journal 46 at 46.

¹⁶⁶ The NSI policy is examined in Chapter 4.2.2. below.
gitimate right to the domain name. On the other hand, the *US Federal Trademark Dilution Act of 1995*\(^{167}\), was explicitly enacted, at least in one view, to deal with the conflicts between domain names and trademarks.\(^{168}\) The trademark legislation may thus deal with some of the types of conflicts between domain names and trademarks, whereas other types of conflicts need another solution.\(^{169}\)

In general, trademark infringement or dilution may be established if use of the domain name can be said to constitute a use of the trademark, i.e. to distinguish goods or services used in the course of trade from other products.\(^{170}\) The domain name is not a trademark *per se*; however, it may be trademark-like. As revealed above, the domain name may serve the same function as a trademark. Nevertheless, merely registering a domain name may not be sufficient conduct to constitute infringement or dilution. Moreover, even posting a web page under the domain name may not be actionable. There is no particular reason to suppose that “cybernauts” happening to surf to the domain name “mcdonalds.com” would associate the site with a source of hamburgers. They can not buy hamburgers at the site, hence there is no confusion between the domain name and the trademark. Moreover, the world is full of individuals named McDonald, any of whom might have registered such domain names with the NSI.\(^{171}\) In other words, the notion of dilution and likelihood


\(^{168}\) Sen. Patrick Leahy said this about the Act; “It is my hope that this antidilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others”. *Cong. Rec.* Dec. 29, 1995, S19312.

\(^{169}\) An example of the wide-held belief that trademarks have protection on the Internet, is the customised Internet search service called MarkWatch. Datalytics, Inc. provides clients with a weekly report of potentially questionable uses of their trademarks on the WWW. Wilder, C., “Trademark protector” (November 25, 1996) *Informationweek* 60 at 60.

\(^{170}\) McKeough and Stewart, *above n. 102* at 464. See Chapter 3.9 above.

\(^{171}\) Burk, *above n. 2.*
of confusion in traditional trademark law does not satisfactorily cover the situation in cyberspace. For example, in the US Intermatic case\(^\text{172}\), the court did not find that the likelihood of confusion requirement was fulfilled. In the reasoning process, the court stated that the domain name “intermatic.com” is similar to the trademark Intermatic. However, there was no similarity between the products and the services that Toeppen and Intermatic provided. Further, there was no evidence of consumer confusion.

Consequently, the carrying over from real space to cyberspace of trademarks, especially weak trademarks, weakens even more the presumption of distinctiveness. In contrast, a site designated with a strong trademark, such as “exxon.com”, seems distinctive whether in real space or in cyberspace.\(^\text{173}\) Moreover, when trademarks are transported to the new medium, Dan L. Burk, at the University of Richmond, suggests that a key factor in analysing the likelihood of confusion of a domain name and a trademark will be the “proximity” of the marks.\(^\text{174}\) In other words, the use of the name McDonalds for hamburgers in real space may not necessarily overlap with the use of the same name for a resource locator in cyberspace. The two uses may be in distinctly different markets. They may also involve very different services, as the major commodity on the Internet is information, rather than hamburgers. In contrast, the use of marks like “MTV” on the Internet may already entail a high likelihood of confusion, as it is associated with entertainment in both real space and cyberspace. Similarly, the trademark “Microsoft” and the domain name “microsoft.com” are likely to be confused. Microsoft sells computers and software, thus there is a close connection between the products and the Internet. Consumers are likely to associate the Internet address with the computer company. Consequently the use of the Internet becomes a natural exten-

\(^{172}\) The Intermatic case, above n. 73. The Intermatic case is examined in Chapter 4.2.3.

\(^{173}\) Burk, above n. 2.

\(^{174}\) Ibid
sion of the service offered in real space. In other words, the marks are more likely to overlap in proximity.\textsuperscript{175}

This is beginning to change, however, as companies begin to utilise their Internet presence to allow customers to order products including fast food delivery of tacos.\textsuperscript{176} Consequently, the real and virtual markets may eventually converge. To date the domain names in dispute have drawn much of their recognition and goodwill from their use as trade or service marks in real space. This may change as commerce on the Internet develops further and marks occur that have acquired their reputation solely through the new medium (so-called cybermarks). Consequently, there may be a need for a new solution and thus new law - cybermark law.\textsuperscript{177}

4.2 The United States - the NSI Policy

Having examined the NSI domain name allocation policy and the intersection between domain names and trademarks in general, it is essential to illustrate the clash between domain names and trademarks by examining some of the cases and settlements resulting from the policy. The vast majority of cases about domain names and trademarks are from the US, hence one has to examine whether there are any flaws in the policy that might explain this.

4.2.1 An introduction to the results of the NSI domain name allocation policy

As a result of the NSI \textit{first come-first served principle}, some persons and companies started “warehousing” domain names. These “cybersquatters” registered domain names such as “deltaairlines.com” and “britishairways.com”, and knew that sooner or later the dormant owners of the well-known trademarks would

\textsuperscript{175} \textit{Ibid}

\textsuperscript{176} Several companies deliver fast food ordered at their Internet site, see for example FasTaco, Texas, USA, at \url{http://www.webcom.com/~fastaco/} (accessed 12 November 1997) who delivers Mexican food.

\textsuperscript{177} The proposal of a cybermark is examined in Chapter 4.7. below.
wake up and realise that they need to go online. Consequently, when they woke up, they found that the most logical domain name ("theircompanyname.com") was taken. This resulted in a number of lawsuits, many of which were legitimate; for example, the Candy-land, Kaplan\textsuperscript{179} and Intermatic\textsuperscript{180} cases. However, the desire to grab the domain name back went to the extreme, and resulted in a reverse domain name hijacking, such as in the Prince case.\textsuperscript{181} The policy also resulted in a widespread sale of second level domain names, such as the Intermatic case, and out-of-court settlements; for example, the McDonalds and the MTV cases.\textsuperscript{182}

4.2.2 The NSI dispute resolution policy

\textsuperscript{178} Intermatic Incorporated v. Dennis Toeppen, above n. 73. See Chapter 4.2.3. below.

\textsuperscript{179} Stanley Kaplan v Princeton Review. Stanley Kaplan and Princeton Review are competitors in the test preparation business. Princeton obtained the domain name “kaplan.com” and posted a WWW page featuring advertisements that promoted Princeton and belittled Kaplan. Kaplan sued for trademark infringement. The suit was ultimately resolved through binding arbitration in Kaplan’s favour. Smedinghoff, above n. 90 at 230.

\textsuperscript{180} See Chapter 4.2.3.

\textsuperscript{181} This was the first cross-border domain name case and was litigated in the UK, see Chapter 4.5.1.

\textsuperscript{182} In the McDonalds case, the writer Quittner registered the “mcdonalds.com” when writing for his column. He registered the domain name only to make a statement regarding McDonalds’ failure to protect their famous name. He offered to surrender the domain name if McDonalds donated some Internet equipment for a US grade school.

In the MTV case, the MTV video jockey Adam Curry organised a WWW site registered as “mtv.com” during his employment period. When he quit his job, MTV demanded that Curry surrender the “mtv.com” site because it carried the designation “mtv”. Curry refused to do so. The parties quietly settled the dispute on March 24, 1995, and it appears that MTV is now in control of the domain name. [WWW - http://www.jmls.edu/cyber/cases/domain2.htm#mtv] (Accessed 5 August 1997) MTV Networks v Curry, 867 F.Supp. 202 (S.D.N.Y. 1994).
Before examining the cases, it is necessary to have an understanding of the NSI dispute resolution policy. It is also important to examine whether the dispute resolution policy has any impact on the increasing amount litigation regarding domain names.

Faced with increasing litigation of domain name disputes and finding itself in the middle of the line of fire, NSI formulated a dispute resolution policy in the event that a third party alleges that the registration of the domain name violates his or her legal rights. Section 5 (a) states that the third party must submit proof of a trademark, either of a US or foreign registration. In addition, the trademark owner must notify the domain name holder, "specifying unequivocally and with particularity that the registration and use of the Registrant's Domain Name violates the legal rights of the trademark owner". Moreover, the trademark owner must provide NSI with a copy of the notice. In other words, the trademark owner must send two letters, one "warning letter" to the domain name holder and a copy of the warning letter together with proof of trademark registration to the NSI.

If the trademark owner has complied with section 5, the procedure continues to section 6. NSI will then determine the "activation date" of the registrant’s domain name. The domain name holder can continue to use the domain name if:

1. the activation date is **before** the date of first use or registration of the trademark; or
2. the activation date is **after** the date of first use or registration of the trademark, and the domain name holder can submit proof of ownership of a registered trademark. The trademark must be registered prior to the earlier of the date of the third party’s notice, or the NSI request for the domain name holder’s proof of ownership. It is also noteworthy that section 6 (c) requires: "the mark provided must be identical to the second-level Domain Name registered to the Registrant".

---

183 NSI’s Domain Name Dispute Policy, *above n. 77.*
If the domain name holder does not comply with (1) or (2), NSI will “assist [the] Registrant with assignment of a new domain name, and will allow [the] Registrant to maintain both names simultaneously for up to ninety (90) days...At the end of the ninety (90) day period of simultaneous use, Network Solutions will place the disputed Domain Name on “hold” status, pending resolution of the dispute”.184

While the domain name is “on hold”, it will not be available for use by any party: section 6 (d). The domain name will also be placed on hold if the domain name holder fails to provide proof of trademark within 30 days (the “30-day letter”), does not accept the assignment of a new name nor relinquish its current name, or fails to take any action at all: section 6 (e).

The parties of the dispute can avoid the domain name being placed on hold by filing a lawsuit. If either the domain name holder or the trademark owner sues the other “in any court of competent jurisdiction in the United States” prior to the domain name being placed on hold, NSI will not cut off the domain name. In such cases, NSI will “deposit control of the Domain Name into the registry of the court”: section 7 (a) and (b).185

These provisions have been harshly criticised. As a result of the dispute resolution policy, the domain name holder is dragged into a dispute. This may happen no matter how legitimate the domain name holder’s use is. Moreover, the risk of losing the domain name is ever-present, even if the domain name holder is not infringing any trademark rights.186 If the domain name holder does not have a

184 NSI’s Domain Name Dispute Policy, above n. 77. Also see Friedman, above n. 62.

185 NSI’s Domain Name Dispute Policy, above n. 77.

trademark registration the domain name will be placed on hold which can cause serious harm. The trademark owner, however, enjoys two options if s/he wishes to have someone’s domain name cut off.

The first option, the courts, is applicable when the possibility of alleging trademark infringement or dilution is present. Otherwise, the courts will dismiss the case. The second option, NSI’s parallel system, may be used against a non-infringing domain name holder. The NSI policy merely says the third party must allege that the domain name “violates the legal rights”, not necessarily trademark rights. Consequently, this permits the challenger to say whatever it wishes. A “small” domain name holder will just drop the domain name and run if a “large” trademark owner uses lawyers and sends a warning letter. Thus, a person may have been legitimately using a domain name for several years before some trademark owner sends a warning letter. Moreover, the challenger may use this policy to attempt to secure a domain name it has no right to. The innocent domain name holder that has received a “30-day letter” from NSI, has little choice but to sue NSI and/or the trademark owner to keep NSI from placing the domain name on hold. However, this result is unfair, as the domain name holder then must bear the burden of initiating a court process, and thus has to convince the court that he or she has a right to use the domain name. In other words, the policy reverses the onus of proof and makes the domain name holder the plaintiff who must bear all the attendant burdens. Further, if a court action is beyond the domain name holder’s means he or she can relinquish any hope of retaining the domain name.

To prevent oneself against such situations, the domain name holder should obtain a trademark registration immediately in order to ob-

---

head of IANA, disagrees. He argues that a registry should not be responsible for verifying that names are free of claims.


tain proof of trademark prior to the earliest date of the warning letter from the trademark owner or the request of proof from NSI. However, as already discussed, not all domain names fulfil the requirements for trademark registration and can not be registered at all. Thus the NSI policy leads to the result that a domain name holder that can not register his/her domain name as a trademark has no protection. Oppedahl comments that the NSI policy “artificially elevates a trademark registration to the special status of being the only way a domain name owner can protect itself”. It is interesting to note that the NSI policy does not accept any common law trademark rights that the domain name holder might possess. On the other hand, NSI accepts both common law trademark rights and registered trademarks the challenging trademark owner might have. This begs the question why there is a difference in standard for trademark owners and domain name holders. One may only assume that NSI decided it was less likely to be sued by a domain name holder than a trademark owner, thus the policy favours the latter. In other words, their decision was a business decision, not a legal or ethical one. This raises another question, should the whole issue have been left to the courts? When placing a domain name on hold, NSI is granting *de facto* preliminary relief in favour of a trademark owner on the mere assertion of a violation. Thus it looks as if NSI is playing court, applying a hybrid form of trademark protection. The question can be raised whether there will be conflicts of interests when a commercial corporation such as the NSI takes drastic actions which usually is the providence of a court.

189 The NSI Domain Name Dispute Policy section 6 (c), above n. 77.

190 Oppedahl, C., “NSI Flawed Domain Name Policy information page”, above n. 188.

191 The NSI dispute policy section 5 (a) provides; “Proof of such a trademark must be by submission of a certified copy, not more than six (6) months old, of a United States Principal or foreign registration...”, above n. 77.

192 For a discussion of this issue, see Chapter 5.4.2.
Another issue is how to interpret NSI’s requirement that “the mark provided [by the domain name holder] must be identical to the second-level Domain Name registered to the Registrant”.\(^{193}\) If “identical” covers identical sounds; for example, phonetic likeness such as “Bali” and “Berlei”, the policy is similar to the notion of likelihood of confusion in trademark law.\(^{194}\) However, Oppedahl has interpreted this phrase to mean that “mere text identicality between a trademark registration and a domain name is evidence that a domain name ‘violates the legal rights’ of the owner of the trademark registration”.\(^{195}\) As a result of this interpretation, CODAK is not “identical” to KODAK. Consequently, an owner of a similar domain name to that of the registrant can not use the NSI policy to allege that the domain name in question violates his or her legal rights.\(^{196}\)

If a domain name is placed on hold, one may ask what kind of harm the suspension may cause the domain name holder. In a worst case scenario, losing a domain name would mean going out of business.\(^{197}\) At least it would cause disruption and monetary expense, and in many cases it would temporarily put a company out of business. For instance, in the *Roadrunner Computer Systems, Inc. v Network Solutions, Inc.*, Roadrunner Computer Systems, Inc.

---

193 The NSI Domain Name Dispute Policy, section 6 (c), above n. 77.

194 In *Berlei Hestia Industries Ltd v Bali Co Inc.* (1973) 129 CLR 353, the phonetic likeness was very strong between trademarks for the same goods which were asked for by name (“Can I have a Berlei bra/Bali bra?”) rather than selected by the customer. The court found that this overrode any written similarity. Thus the sounds of trademarks have often been relevant in trademark law cases. See McKeough and Stewart, above n. 102 at 462.

195 Oppedahl, “NSI Flawed Domain Name Policy information page” above n. 188.

196 In comparison, see the gTLD-MoU proposal, Chapter 5. The gTLD-MoU approach is more similar to the likelihood of confusion requirement in trademark law.

(RCS)’s president stated that loss of the domain name “would be disastrous” and that one-fourth of the customers would be lost, in part because the company would have had to change its email address. Moreover, in the complaint, RCS argued that

NSI is on Notice that RCS is an Internet Service Provider having contracts with numerous individuals to provide access for those individuals to the Internet, and that discontinuation of the roadrunner.com domain will materially and negatively effect RCS’s ability to provide these services, either resulting in a breach of RCS’s contracts with its subscribers or in a material increase in the price of fulfilling RCS’s contract obligations.

Domain name holders have sued NSI because they believe that they have a legitimate right to use their domain name. The Roadrunner case is only one of several court cases that have occurred in connection with the NSI policy. Another example is the Clue case.

198 Oppedahl, “Analysis and Suggestions Regarding NSI Domain Name Trademark Dispute Policy” [WWW - http://www.patents.com/-nsi/iip.sht] (Accessed 5 August 1997). The reason why the company has to change the email address, is because when the domain name is “roadrunner.com”, the email address usually is “personname@roadrunner.com”. Hence when the domain name is on hold, the email address does not function.


200 The Roadrunner case, above n. 199.

201 There is a list of lawsuits against NSI at OppedahFs “NSI Flawed Domain Name Dispute Policy information page”, above n. 188.

202 Clue Computing, Inc. v Network Solutions, Inc. [WWW - http://www.-patents.com/clue/clue.sht] (Accessed 16 September 1997) and [WWW - http://www.clue.com/legal/nsi/complain.html] (Accessed 18 September 1997), above n. 64. The court ordered NSI not to put the domain name on hold. Note that there are three Clue cases, above n. 64. On February 1, 1996, NSI informed Clue that its use of “clue.com” may infringe on Hasbro’s trademark. Clue initiated a lawsuit against NSI for breach of contract. NSI responded by filing an interpleader action against Clue and Hasbro (28 U.S.C. paragraph 1335) claiming that it is an “impartial and unbiased stakeholder, has no interest in the
To date, the results have been that the domain name holders get to detain their domain names, either because NSI is enjoined from placing the domain name on hold, or because NSI, to avoid being enjoined, agreed not to cut it off.\(^\text{203}\)

The arbitrary nature of the NSI policy is highlighted in *Prince plc v Prince Sports Group, Inc.*\(^\text{204}\) This case was the first cross-border domain name dispute. The NSI policy states that NSI will not place a domain name on hold if a lawsuit is filed in "any court of competent jurisdiction in the United States".\(^\text{205}\) However, the Prince company from the UK filed a suit in a court in the UK, hence they did not comply with the requirement in the policy. Oppedahl comments that the Prince company from the US fulfilled all the requirements for placing Prince from UK’s domain name on hold. Nevertheless, NSI did not put it on hold.\(^\text{206}\) What does this mean? Oppedahl suggests that NSI might have a “secret policy” of sometimes not cutting off domain names even though the formal requirements of its policy are met. Thus there is an open question whether one may sue in a US court only, or in any jurisdiction in the world.

In conclusion, there are serious problems with the current NSI dispute resolution policy. The policy fails to take into account any rights that one might have to a trademark or a service mark resulting from common law usages. Second, the policy fails to address weak

---

\(^{203}\) Oppedahl, “NSI Fourth Domain Name Policy Leaves Owners With Few Options”, *above n. 186.*

\(^{204}\) *Prince plc v Prince Sports Group, Inc.* [http://www.prince.co.uk/-judge.htm] (Accessed 25 August 1997). The *Prince* case will be revised in Chapter 4.5.1.

\(^{205}\) See the NSI policy, section 7 (a), *above n. 77.*

\(^{206}\) Oppedahl, “NSI Flawed Domain Name Dispute Policy information page” *above n. 188.*
trademarks such as Acme, Eagle, American or Genesis.\textsuperscript{207} Third, there is no process for dealing with likelihood of confusion cases. Several organisations have held numerous conferences and meetings over the past few years to discuss the domain name problem and other issues regarding the Internet. This paper examines one proposal, the gTLD-MoU, in Chapter 5.

\textit{Having described the NSI dispute resolution policy, the following sections under Chapter 4.2. will deal with some of the cases and out-of-court settlements.}

\subsection*{4.2.3 The Intermatic case}

As an illustration of domain name grabbing, the case \textit{Intermatic, Inc. v Dennis Toeppen}\textsuperscript{208} highlights the issue of domain name hijacking of famous trademarks. In this case, the court granted a summary judgement in favour of the plaintiff for the defendant’s use and registration of the domain name “intermatic.com”. The defendant, Mr Toeppen, had registered not only “intermatic.com”, but approximately 240 domain names, including well-known business names such as “britishairways.com”, “deltaairlines.com” and “ussteel.com”.\textsuperscript{209} The owner of the trademark “Intermatic” thus sued

\begin{footnotesize}
\begin{enumerate}
\item Frank, \textit{above n. 22.}
\item The \textit{Intermatic Incorporated v. Dennis Toeppen}, \textit{above n. 73.} The Intermatic court wrote a 32 page opinion which opened by saying “Welcome to cyberspace! This case presents the Court with the increasingly important issue of whether and how federal and state trademark laws apply to govern names selected by users for their Internet website. As the Internet grows in prominence as a venue for business, the courts will be called upon to apply traditional legal principles to new avenues of commerce. This is such a case”. \textsuperscript{208} The \textit{Intermatic, Inc. v Dennis Toeppen, above n. 73.} The court actually calls Mr. Toeppen a “cyber-squatter”. Then the court defines “cyber-squatters” as: “individuals [who] attempt to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing goodwill of the trademark”. See also “Current Developments” “Domain Name Violates Trademark Dilution Act, District Court Rules” (1996) 13 (11) \textit{The Computer Lawyer} 20 at 20. \textsuperscript{209}
\end{enumerate}
\end{footnotesize}
Toeppen, alleging trademark infringement, trademark dilution and related causes of action.\(^{210}\)

However, the problem was the apparent inapplicability of substantive law to the conduct. The court ruled that the cause of action under the *Lanham Act* would not stand, because there was no likelihood of confusion between the products offered by the plaintiff and the defendant. Moreover, Toeppen was not engaged in any commercial activity. This illustrates the issue of whether traditional trademark law is applicable to domain name disputes.\(^ {211}\) The *US Federal Trademark Dilution Act*\(^ {212}\) explicitly limits itself to commercial activity. The court tried to find something “commercial” in Toeppen’s conduct. The court first stated that “the use of the first level domain designation “.com” does not in and of itself constitute a commercial use”. Then the court went on to say that

Toeppen’s intention to arbitrage the “intermatic.com” domain name constitutes a commercial use... Toeppen’s desire to resell the domain name is sufficient to meet the ‘commercial use’ requirement of the Lanham Act.

The court thus ordered that the domain name should be transferred to the trademark owner.\(^ {213}\)

4.2.4 The Roadrunner case

---


\(^{211}\) See Chapter 4.1.3. above.

\(^{212}\) *US Federal Trademark Dilution Act*, above n. 126.

\(^{213}\) Critics argue that the transfer of the domain name relief did not follow from the Federal Dilution Act. See Oppedahl, “Remedies in Domain Name Lawsuits: How is a domain name like a cow?”, above n. 66. This will be discussed in Chapter 4.6. below.
Frequently, there are two businesses (or more) that desire the same domain name, and only one of them has trademark rights in relation to the domain name. A conflict might occur if the one without trademark rights registers the name as a domain name under the first come-first served principle. This occurred in the *Roadrunner case* and the *Candyland case*.\(^{214}\)

In the *Roadrunner case*\(^ {215}\), Roadrunner Computer Systems, an Internet service provider, held the domain name “roadrunner.com”. Warner Bros., which holds a trademark on the Road Runner cartoon character, contacted Roadrunner Computer Systems, Inc. and demanded they should produce their own trademark. Roadrunner then obtained a trademark registration in Tunisia. However, NSI said that the registration was obtained too late and decided to put the domain name on hold.\(^ {216}\)

### 4.2.5 The Wire/Wired settlement

Another scenario occurs when two domain names are confusingly similar. This happened in the out-of-court settlement between Wire

---

\(^{214}\) The *Candyland case* [WWW - http://www.jmls.edu/cyber/cases-domain1.html#candyland] (Accessed 5 August 1997). *Hasbro, Inc. v Internet Entertainment Group, Ltd.*, No. C96-130WD (W.D. Wash. Feb. 9, 1996). In the *Candyland case*, Hasbro, Inc., a large toymaker, was the owner of the trademark “Candyland”. The defendants, Internet Entertainment Group, had registered the domain name “candyland.com” for a sexually explicit Internet site. The court found that the use of the domain name was likely to dilute the value of Hasbro’s Candyland mark, and ordered that the defendants should remove all content from the site. See also Friedman, *above n. 62*.

\(^{215}\) Note that there are two Roadrunner cases. The first was *Roadrunner Computer Systems, Inc. v Warner Bros*. This is an out of court settlement [WWW - http://www.wired.com/wired/4.10/updata.html] (Accessed 16 September 1997). The second case was *Roadrunner Computer Systems, Inc. v Network Solutions, Inc.*, *above n. 199*.


77
and Wired.\textsuperscript{217} Wire, a computer network devoted to women’s issues, registered the domain name “wire.net”. Wired, a cyberspace magazine, holds the domain name “wired.com”. Wired complained about the domain name used by Wire. Rather than litigating the issues, Wired contacted Wire and asked them to change their name. The parties settled with Wire agreeing to change its name to Women’s Wire and its domain name to “wwire.net”.\textsuperscript{218} It is worth noting that they changed not only their domain name, but also their business name in real space. This helps minimise any likelihood of confusion. The dispute is interesting, as it is an early precursor to the kind of cybermark conflicts that will arise in the future.\textsuperscript{219} The Wired/Wire settlement it is not about the appropriation of a well-known trademark from real space, but the confusing similarity between two cyberspace-based marks.\textsuperscript{220}

4.2.6 The US Federal Trademark Dilution Act

One of the first suits under the US Federal Trademark Dilution Act of 1995, was filed by Avon Products.\textsuperscript{221} Avon is a giant personal products and door-to-door merchandiser. The company could not obtain the domain name “avon.com” because Carnetta Wong Associates had previously registered it under the NSI policy first come-
first served. According to Avon, Wong’s purpose in registering “avon.com” was to prevent Avon from establishing a domain name using that domain until Avon paid the defendant a sum of money satisfactory to Wong. Avon sought the transfer of the domain name and the court granted the transfer because of the dilution of the trademark owner’s rights. It is interesting to note that the dilution action was successful notwithstanding the lack of the use of the domain name as a trademark.222

As mentioned in Chapter 3 above, when using the US Dilution Act one need not prove a likelihood of confusion. Nevertheless, it is worth noting that the US courts that have applied the Act have adopted a six factor blurring test set forth in the case Mead Data Central Inc. v Toyota Motors Sales U.S.A. Inc.223 Thus critics allege that the Mead Data test dilutes the US Dilution Act. The Mead Data factors are similar to those commonly used to determine likelihood of confusion.

Having examined the NSI dispute resolution policy and the cases in connection with the policy, one may ask why the domain name litigation rate is so high in the US. As seen, in all domain name cases trademark law has been applied to the conflict. Breach of intellectual property rights has been alleged, successfully and unsuccessfully. One reason why there has been so much uncertainty regarding domain name cases and settlements in the US might be that trademark law is not suited to solve Internet domain name conflicts. Another reasons might be the NSI policy’s flawed emphasis on trademark

222 In Australia, it would seem that a domain name would have to be “used” as a trademark if the complainant was to succeed in a case with similar facts as the Avon case, above n. 221.

223 The Mead Data Central Inc. v Toyota Motors Sales U.S.A. Inc. 875 F.2d 1026, 1035 (2d Cir. 1989).

Judge Sweet in the Mead Data case identified six factors as relevant to the dilution by blurring inquiry: the similarity of the marks, the similarity of the products covered by the marks, the sophistication of consumers, predatory intent, the renown of the senior mark, and the renown of the junior mark. Shapiro, above n. 137. See also Chapter 3 above.
rights. The NSI policy is not sufficient or adequate. Thus it is essential to examine other policies to discover whether there are more feasible approaches to the domain name disputes.

4.3 The United Kingdom - the Nominet UK policy

The domain name “co.uk” is one of the most common domain names after the “.com”.\(^{224}\) Hence it is important to have an overview of the Nominet UK’s dispute resolution policy. Also, the first legal ruling on the domain names in the UK, the case Pitman Training Limited \(v\) Nominet UK\(^{225}\), will be examined.

The Nominet UK has a “hands-on” approach to domain name disputes, similar to that of the NSI.\(^{226}\) The dispute resolution policy provides that when a third party is “laying claim to a stronger right to register it [i.e. the domain name under a sub-domain of the “.uk” TLD], Nominet will assist the parties”. Nominet will first investigate, and if investigation does not lead to a “mutually acceptable resolution of the dispute”, Nominet will consider whether the domain name should be suspended. If a party is dissatisfied with Nominet’s decision to suspend or not to suspend, Nominet will refer the suspension to an independent expert for a written recommendation. On receipt of the expert’s recommendation, Nominet will reconsider its decision. If a party is dissatisfied with Nominet’s final decision, Nominet will offer the parties to enter into a mediation agreement.\(^{227}\) If mediation does not solve the dispute or one of the parties refuses to enter into mediation, “the dissatisfied party will remain in a position to seek advice from its lawyers about pursuing its case by litigation in the courts or... arbitration”.\(^{228}\) Once more,


\(^{225}\) The Pitman case, above n. 224.


\(^{227}\) The “Nominet Alternative Dispute Resolution Service” administered by the Centre for Dispute Resolution, above n. 226.

\(^{228}\) The Nominet Dispute Policy section 11, above n. 226.
one may ask whether it is desirable that the domain name disputes are resolved by the same entity as the one that grants them.\footnote{See Chapter 5.4.2. "Should the dispute resolution be left to the courts?".}

The *Pitman* case raised questions about the rights acquired by someone who registers a domain name. The problem was, that both the plaintiff Pitman Training Ltd. (PT) and the defendant Pearson Professional Ltd. (PP) were entitled to use for their respective trading purposes the name “Pitman”. One of the divisions under Pearson Professional Ltd. is Pitman Publishing. PP’s main business was publication of books and electronic publications. PT performed training business. PP registered the domain name “pitman.co.uk”. However, PP did not make use of the domain name. Later, when PP attempted to connect its WWW page to the “pitman.co.uk”, PP discovered that the domain name had been re-delegated to PT. PT had actively used the domain name for some months. PT applied for an interlocutory relief, and an order was made restraining Nominet from suspending the domain name and PP from using it. In this case, the issue was whether PT, pending trial, should have an injunction against PP. The judge found that the plaintiff could not obtain an interlocutory relief against the defendant and dismissed the application.

There has not been as plentiful litigation in the UK regarding the domain name “co.uk” as in the US under the NSI policy. Thus one may ask whether the Nominet policy provides a better approach to domain name disputes. However, to NSI’s defence; the NSI administers the highly desired “.com” TLD which is not an uncomplicated task. The Nominet administers the “.co.uk”, which is not as attractive as the “.com”. Hence it is necessary to examine another policy with a different approach from the NSI and Nominet.

### 4.4 Australia - the Melbourne IT policy

*The Melbourne IT policy is an example of a “hands-off” approach to domain name disputes. As mentioned above, Melbourne IT re-*
vokes a domain name "where a court of competent authority deter-
mines that the domain name should not be allocated to the appli-
cant...".\textsuperscript{230} In other words, it leaves the disputes to the courts.

At present, the Sydney 2000 case is the only case regarding domain
names in Australia.\textsuperscript{231} The domain name “sydney2000.net” was
registered by the Asia Pacific Internet Company (APIC) with the
NSI. The Australian Sydney Organising Committee For The Olympic
Games (SOCOG) proposed to take action under the Sydney 2000
Games Protection Act,\textsuperscript{232} the Trade Practices Act for “misleading
and deceiving” and common law for “passing off”.\textsuperscript{233} The action
raised a number of issues.\textsuperscript{234} The Sydney 2000 Games Protection Act
was enacted after the NSI registered the domain name. Thus the
question was, can a government legislate to override domain names
issued by the NSI? A complicating factor was that Sydney 2000 has
a further meaning beyond the Olympic Games. Sydney 2000 is the
postcode of the Sydney business district. This in itself could represen-
ta commercial value beyond the Olympics.

There has been little or no litigation of domain name conflicts in
Australian courts. Moreover, there have not been any conflicts be-
tween domain names and trademarks. The Melbourne IT has the
most efficient and effective domain name allocation policy. Con-
flicts between domain names and trademarks have been solved


\textsuperscript{231} For The Sydney 2000 case see Barry, G., “Olympic Battle Over Domain
Name” [WWW - http://www2.ucsc.edu/people/booloo/iilist/May97/0-

\textsuperscript{232} The Sydney 2000 Games (Indicia and Images) Protection Act 1996
(C’wth) - No 22 of 1996 [WWW -http://www.austl ii.edu.au/do2/-
disp/pl/au/legis/cth/consol_act/s2000gaipa1996378/s12.html] (Ac-
cessed 8 November 1997).

\textsuperscript{233} Barry, above n. 231.

\textsuperscript{234} One limitation in this case, is the fact that the Act is limits its jurisdic-
tion to Australian territory. Hence one is outside the scope of the Act if
one register Sydney 2000 in another country; e.g.
“sydney2000.net.nz”.
through negotiations and preventive actions. Furthermore, it seems like a “hands-off” approach to domain name conflicts is the best: when the collision is unavoidable, the courts solve the conflict and the domain name registry acts accordingly.
4.5 Two possible defences against allegations of trademark infringement and dilution - groundless threat and the doctrine of trademark misuse

Having examined the domain name dispute policies and the results in the US, the UK and Australia, this section will focus on the defences against allegations of breach of intellectual property rights.

4.5.1. The United Kingdom

In the UK, *Prince plc v Prince Sports Group, Inc.* is an illustrative case.\(^{235}\) The case is based upon the *UK Trade Marks Act of 1994* s 21 on groundless threats of infringement. Section 21 is the counterpart of the Australian TM Act s 129.

In the *Prince* case, the US company Prince Sports Group, Inc. (Prince US) sent a letter to the UK company Prince plc. (Prince UK). Prince US is known for the making of tennis racquets, whereas Prince UK is an IT services company. Prince US alleged that the domain name “prince.com” should be transferred to Prince US. Prince UK registered the domain name “prince.com” in 1995. Prince US asserted that they were the owners of a famous trademark, used in connection with sports equipment for the past 20 years in the US, and hence Prince UK’s use of the domain name “prince.com” on the Internet prevented Prince US from registering “its house mark and trade name as a domain name” and thus constituted infringement and dilution of their trademark. Prince US asserted that the matter could be solved by an assignment of the “prince.com” domain name to them, under the NSI policy procedure, to avoid litigation.\(^{236}\)

However, under the *UK Trade Marks Act of 1994* s 21, it is unlawful for an owner of a trademark to make unjustifiable threats of trade-

\(^{235}\) *The Prince plc v Prince Sports Group, Inc.*, above n. 204.

\(^{236}\) *The Prince case*, above n. 204. Prince US claimed that “this matter can be amicably resolved by an assignment of the PRINCE.COM domain name to Prince Sports Group, Inc., in accordance with the procedures of NSI and an agreement not to use PRINCE as a part of any new domain name you may select”.

mark infringement. Prince UK thus commenced proceedings against Prince US for injunctions and damages asserting that the threat was unjustifiable. Section 21 provides that:

(1) Where a person threatens another with proceedings for infringement of a registered trade mark...any person aggrieved may bring proceedings for relief under this section.

(2) The relief which may be applied for this is any of the following:-

(a) The declaration that the threats were unjustifiable...

and the plaintiff is entitled to such relief unless the defendant shows that the acts in respect of which proceedings were threatened constitute (or if done would constitute) an infringement of the registered trade mark concerned...  

The judge dealt with the question whether the letter was a threat of “proceedings for infringement of a registered trade mark”. He construed the letter, in accordance with the approach laid down by authority, as how it would be understood by an ordinary reader. He concluded that the letter, in connection with the other facts, constituted a threat within the meaning of section 21.  

The Prince case illustrates that s 21 may be used as a defence against trademark owners who try to expand their trademark rights to allow them to seize the domain name from legitimate domain name holders. Hence when a domain name holder has a legitimate right to own a domain name and was the first to register it, then the trademark owner has no better right to own it and has only

---

237 The Prince case, above n. 204.
238 The Prince case, above n. 204.
239 The Prince case, above n. 204. In his judgement, Mr Justice Neuberger issued warnings to trademark owners. He said that “...persons who have the privilege of a UK registered trade mark should not abuse that privilege...”, moreover, he should “...consider with care whether he has a case...”.
him/herself to blame if the proceedings result in relief being granted against him/her.\textsuperscript{240}

4.5.2 Australia

In Australia, the TM Act s 129 is the counterpart of s 21 in the UK Act. The relevant subsections in s 129 provide:

(1) If a person threatens to bring an action against another person ... on the ground that the threatened person has infringed:

(a) a registered trade mark; or...any person aggrieved by the threat ... may bring an action...against the person making the threat ... 

(2) The purpose of the action is to obtain from the court:

(a) a declaration that the defendant has no grounds for making the threat...\textsuperscript{241}

This section may be pleaded as a defence in the same fashion as illustrated in the \textit{Prince case}.

4.5.3 The United States

In the US, there is no provision in the \textit{Lanham Act} similar to the UK s 21 and the Australian s 129.\textsuperscript{242} However, the question can be raised whether the doctrine of trademark misuse may be used as a defence similar to the groundless threat defence.

The doctrine of trademark misuse prohibits a trademark owner from using its trademark in a manner that violates the public policy embodied in the grant of a trademark.\textsuperscript{243} Courts may extend the broad equitable doctrine of trademark misuse to prevent trademark owners


\textsuperscript{241} The Trade Marks Act 1995, above n. 94.

\textsuperscript{242} Davidson, S.J. and Engisch, N.A., "‘Trademark Misuse’ in Domain Name Disputes" (1996) 13 (8) \textit{The Computer Lawyer} 13 at 17.

\textsuperscript{243} Davidson and Engisch, above n. 242 at 14.
from complaining unjustifiably to the NSI that their trademark rights entitle them to possess a domain name previously granted to another party under circumstances where the other party’s domain name does not constitute true trademark infringement or an unlawful dilution of a famous trademark.244

According to the trademark misuse case United States Jaycees v Cedar Rapids Jaycees245, trademark misuse will be shown where the trademark owner “has dealt unjustly with the defendant in the very transaction upon which its cause of action is based”.246 The courts have yet to hold that the holder of a validly issued domain name may defend a charge of trademark infringement by claiming that the trademark owner has misused its trademark. However, the Prince case in the UK is an argument for the possibility that the trademark misuse doctrine could be used as a defence. Thus, where a domain name holder has a legitimate right to its domain name, and where the trademark owner is acting inequitably and is attempting to use its trademark to secure rights beyond those granted by trademark law, there should be no barrier to applying the misuse doctrine.247 In effect, the doctrine of trademark misuse operates in a similar manner to s 21 in the UK and s 129 in Australia, and thus may be used as a defence against “reverse domain name hijacking”.

4.6 Remedies in domain name versus trademark lawsuits

244 Davidson and Engisch, above n. 242 at 14.
246 Quoted in Davidson and Engisch, above n. 242 at 16.
247 Davidson and Engisch, above n. 242 at 17. As a counter-argument, one may allege that the US Noerr-Pennington doctrine (which provides that parties have a First Amendment right to petition the government) should not apply to a party's activities before a private body such as the NSI.
Having looked at the intersection between domain names and trademarks, and finding that trademark law is currently used to solve conflicts between domain names and trademarks, this section will examine the remedies in domain name versus trademark lawsuits. Trademark owners have requested not only cease and desist relief, but also transfer of domain name relief in trademark infringement cases. The question is, if a trademark owner succeeds in proving trademark infringement by a domain name holder, does it follow logically that the court should order that the domain name be transferred to the trademark owner as remedy?248

Oppedahl has criticised several US cases where the courts have transferred the domain name to the trademark owner.249 His main argument is that the courts do not bother to explain where they find authority to grant the remedy of ordering that the domain name be handed over.250 When analysing three cases where the courts or-


249 There is no remedy in trademark law or dilution law that calls for transfer of a domain name. See Chapter 2.2. about the nature of a domain name. Oppedahl, “Remedies in Domain Name Lawsuits: How is a domain name like a cow?”, above n. 66.

250 Oppedahl, “Remedies in Internet domain name trademark lawsuits”, above n. 210. Oppedahl points out that in none of the three cases, Actmedia, Inc. v Active Media Int’l Inc., 1996 WL 399707 (N.D. Ill. 1996), Intermatic Inc. v Toeppen, above n. 73, Panavision Int’l L.P. v Toeppen, 945 F.Supp. 1296, USPQ2d (C.D. Cal. 1996), did the court bother to explain where it found the authority to grant the remedy of ordering that the domain name be handed over. See the Intermatic case in Chapter 4.2.3. above. In the Actmedia case, Actmedia Inc. went to the NSI to register the domain name “actmedia.com”, and found that the domain name was already registered by Active Media Int’l Inc. The court found that the domain name holder’s actions constituted trademark infringement and ordered that the domain name be given over to the plaintiff. In the Panavision case, the Panavision Int’l L.P. went to register the domain name “panavision.com”, only to find that the domain name was registered by Mr Toeppen. The court found that the trademark was “famous” under the Federal Trademark Dilution Act, and that Toeppen’s activity was “commercial”, and ordered a transfer of the domain name.
dered a transfer of the domain name, one finds that in the three cases, Actmedia, Intermatic and Panavision, the trademarks are truly unique.\textsuperscript{251} None of them can be found in a dictionary. Moreover, there seems to be a factor that the domain name holder has registered numerous domain names corresponding to “famous” trademarks.\textsuperscript{252} Another relevant factor is whether the domain name holder is doing anything with the domain name.\textsuperscript{253} With this in mind, Oppedahl suggests that a transfer of domain name relief is appropriate only if the trademark being asserted is unique or coined.\textsuperscript{254} Otherwise the first come-first served principle should be the ruling principle, thus the plaintiff should be denied a remedy and should be encouraged to select a different domain name.

4.7 The proposal of a cybermark

Having looked at the current domain name allocation and dispute policies, this section will examine one possible solution, the proposal of a cybermark.

A new branch of intellectual property law, namely the cybermark, has been proposed. A cybermark is a trade name or domain name that has acquired reputation based entirely on its Internet activities.\textsuperscript{255} Disputes between cybermarks, such as the Women’s Wire

\textsuperscript{251} Oppedahl, “Remedies in Domain Name Lawsuits: How is a domain name like a cow?”, above n. 66. Oppedahl informs that searches of online databases show but a single trademark owner for the trademarks, in each case the plaintiff in the action. Searches of directories of corporations show few or no other companies named for the mark.

\textsuperscript{252} In the Intermatic and Panavision cases, Mr Toeppen had registered more than 200 domain names.

\textsuperscript{253} In the Toeppen cases, much attention was paid to this question. The Federal Trademark Dilution Act, above n. 126, requires that there is “commercial activity”, hence the Act should not be applicable to a passive domain name holder. See Chapter 4.2.6. above.

\textsuperscript{254} Oppedahl, “Remedies in Domain Name Lawsuits: How is a domain name like a cow?”, above n. 66.

\textsuperscript{255} Flint, D., “Internet Domain Names, Proposal for a cybermark.” (1997) 13 (3) Computer Law & Security Report 163 at 163. See also Houri-
and Wired Magazine case, will continue to occur increasingly as commerce on the Internet becomes more common.\textsuperscript{256}

The UK solicitor David Flint suggests that the trademark should meet certain criteria and then be considered a cybermark. He suggests that use on the Internet of a cybermark that fulfils these criteria should not be considered as a trademark infringement.\textsuperscript{257} One of the criteria that Flint suggests is that the owner of the WWW page should have a legal right to use the mark in the territory in which the server was situated, and should provide evidence of such entitlement if required. The mark should be either a word normally occurring in the language used on the WWW site or refer to goods and/or services offered by the owner of the WWW page. Moreover, Flint suggests that the server should be based in the same country as the owner of the WWW page, unless the owner can establish a \textit{bona fide} reason why the WWW page is situated in another country. This will avoid servers being situated in territories with less restrictive rules than a party is subject to in his or her home country. Furthermore, the use of the mark should not be directed specifically at readers situated in another territory unless the owner owns rights to such a mark in the other territory.\textsuperscript{258}

In conclusion, it seems possible that a form of cybermark law may develop in the future preventing the use of a domain name which is “substantially identical” or “deceptively similar” to another domain name in cyberspace.\textsuperscript{259} When the Internet provides a stable and predictable environment for business and commerce, cybermark law

\textsuperscript{256} Burk \textit{above n. 2}.

\textsuperscript{257} Flint, \textit{above n. 255} at 166. See also Fair and Delabaere, \textit{above n. 165} at 47.

\textsuperscript{258} Flint, \textit{above n. 255} at 165.

\textsuperscript{259} Fair and Delabaere, \textit{above n. 165} at 47.
may evolve. \textsuperscript{260} Without a cybermark businesses will continue to be subjected to costly legal suits at the behest of unknown third parties in territories where they were unaware of such third parties' existence or conflicting rights. \textsuperscript{261} An internationally valid cybermark would lift the domain name disputes to the international level. Consequently, the DNS would have its own intellectual property law, separated from the traditional trademark law. However, there is need for a stable system of governance to successfully implement a new intellectual property law right on the Internet.

\textsuperscript{260} Currently, disputes between deceptively similar domain names would need to be determined under local law. See Hourigan, \textit{above n. 255} \textsuperscript{255}, who points out that this would place a complainant in a difficult position of having to enforce its rights in multiple jurisdictions. See Chapter 6 below for different models for dealing with Internet governance at the international level.

\textsuperscript{261} Flint, \textit{above n. 255} at 166.
First we shape our structures, 
and afterwards they shape us

-- Winston Churchill.

Having dealt with the proposal of a cybermark, this chapter will consider another possible solution to the current problems in the DNS and the inconsistencies between domain names and trademarks - the gTLD-MoU proposal.

Aims of chapter 5
The aims of Chapter 5 are to:
* thoroughly analyse the gTLD-MoU proposal of seven new gTLDs
* examine the CORE-MoU proposal
* examine the proposal of Administrative Domain Name Challenge Panels, and discuss whether domain name disputes should be left to the national courts of jurisdiction.

5.1 Background on the gTLD-MoU
Recently, attempts have been made to stop NSI's monopoly of the domain name registration in the most popular TLD, "\texttt{.com}". One attractive development, is the gTLD-MoU proposal. The proposal was a result of the International Ad Hoc Committee's (IAHC) Final Report, implemented by the Memorandum of Understanding on the Generic Top-Level Domain Name Space of the Internet Domain
Name System (gTLD-MoU). The Final Report\textsuperscript{262} was issued on February 4, 1997 and the gTLD-MoU\textsuperscript{263} was established on February 28, 1997.

As a basic framework, the “Postel Draft” was used. Jon Postel, Executive Director of the IANA, had circulated a proposal that was referred to as the Postel Draft.\textsuperscript{264} The Internet Society then decided to undertake the domain name problems using this draft. In October, 1996, the Internet Society formed the IAHC. The committee was selected by the World Intellectual Property Organisation (WIPO), IANA, International Telecommunication Union (ITU), IAB, International Trademark Association (INTA) and ISOC.\textsuperscript{265} The initial signatories of the document were the IANA and the ISOC. They have been joined by representatives from industry, government and other organisations, and the process of endorsement is still going on. The ITU acts as a depository for the gTLD-MoU and publishes the list of signatories.\textsuperscript{266} To date (13 January, 1998), 193 entities have signed the gTLD-MoU, including Telstra Australia, Melbourne IT

\begin{itemize}
  \item[\textsuperscript{264}] The Postel Draft is available at ftp://ds.internic.net/Internet-drafts/draft-postel-iana-itld-admin-02.txt. First accessed 28 August, 1997. Second time revised on 8 November, 1997, then the document was deleted.
  \item[\textsuperscript{266}] The gTLD-MoU section 4 provides that “the depository of this instrument shall be the Secretary-General of the International Telecommunication Union”. Furthermore, (a) to (c) define the role of the depository, above n. 263.
\end{itemize}
and the Internet Society of Australia, but the gTLD-MoU has not yet entered into force.\textsuperscript{267} Interestingly, several US entities have signed the MoU, in spite of the general opposition against the gTLD-MoU in the US.\textsuperscript{268}

The gTLD-MoU will provide an instrument for signatories to advise on future policy evolution of the global DNS. In a legal context, however, the question is what gives the gTLD-MoU force: contract law, private international law or public international law? In general, a Memorandum of Understanding is an increasingly preferred instrument of co-operation, less formal than bilateral and multilateral international agreements. As a general definition, international law theorist Anne-Marie Slaughter defines a MoU as an agreement “whereby two or more regulatory agencies set forth and initial the terms of an ongoing relationship. MoUs are not treaties; they do not engage the executive or the legislature in negotiations, deliberation, or signature. They affirm existing links among regulatory agencies based on their common functions and commitment to the solution of problems”.\textsuperscript{269} According to the gTLD-MoU preamble, the document provides an “international policy framework” through the establishment of a “self-regulatory structure under a voluntary MoU”. However, the gTLD-MoU is a policy intended to be binding on the activities of the registrars and the SLD name holders within the gTLD.\textsuperscript{270} In other words, it constitutes both a private international law contract of association and a form of public international administrative regulatory regime.\textsuperscript{271} The gTLD-MoU is an interesting


\textsuperscript{268} The opposition against the gTLD-MoU will be revised in Chapter 5.5. below.


\textsuperscript{270} See Chapter 5.3., regarding the “Council of Registrars” (CORE). CORE is the entity comprising registrars for domain names under the new gTLDs. Visit http://www.core.gtld-mou.org.

\textsuperscript{271} Stoodley, above n. 23 at 510.
hybrid because of the mix of sovereigns and non-sovereigns signing it. It brings public and private actors together in a corporatist style international governance structure.\textsuperscript{272}

If the gTLD-MoU is a contract, however, the question is which country's laws will govern the contract. Will Swiss law govern the gTLD-MoU? Regarding the CORE, the CORE-MoU art. 8 (d) states: "This CORE-MoU shall be governed by the laws of Switzerland". Art. 8 (e) refers disputes arising out of the CORE-MoU to UNCITRAL arbitration under Swiss law.\textsuperscript{273} However, there is no such provision in the gTLD-MoU. Another issue which arises is, on the basis of which laws will the dispute resolution be adjudicated? Further, how will the signatories to the gTLD-MoU be bound by changes? What will keep them bound to changes in the future? Stability is crucial in this area, thus these questions should be addressed before the gTLD-MoU enters into force.

When will the gTLD-MoU enter into force? The gTLD-MoU section 11 (b) provides that the "MoU shall enter into force from the date that it has been signed by both IANA and ISOC". However, if one examines the list of signatories and considers the important bodies that are missing, it indicates that the plan might be difficult to implement.\textsuperscript{274} Although several Internet organisations and societies from countries all over the world have signed the document, the most important Internet players, the engineers that run the root server system, have not signed. Both the IETF and the IESG are missing.\textsuperscript{275} Nonetheless, the gTLD-MoU process is scheduled to be-

\begin{footnotesize}
\begin{footnotes}
\textsuperscript{272} Fitzgerald, B., "Navigating Cyberspace: Frontier Land or Legal Minefield?" (unpublished paper, presented at the Australasian Law Teachers Association Conference, Sydney, Australia, 4 October, 1997).


\textsuperscript{274} Signatories to the gTLD-MoU, above n. 267.

\textsuperscript{275} There was a discussion on the mailing list "gtld-discuss" regarding this issue. Some participants argued that the fact that IETF and IESG are missing, shows that the gTLD-MoU is in for rough times ahead. Others
\end{footnotes}
\end{footnotesize}
gin operation on 15 February 1998, and the new CORE system is scheduled to be fully operational by 30 September, 1998.

5.2 The new gTLDs

5.2.1 Introduction to the seven new gTLDs

One interesting change, is the proposal for seven new generic top-level domains (gTLDs). The new gTLDs suggested are added to the root of the domain name system (DNS) in addition to the existing ones. The new gTLDs and the intended fields of use are:

- "firm" for businesses and firms
- "shop" for businesses offering goods to purchase
- "web" for entities emphasising activities related to the WWW
- "arts" for entities emphasising cultural and entertainment activities
- "rec" for entities emphasising recreation and entertainment activities
- "info" for entities providing information services
- "nom" for those wishing individual or personal nomenclature.

The seven broad gTLD categories chosen were selected as a synthesis of public comments, previous proposals and contributions. For replied that neither the IETF nor the IESG have any legal personality, and thus cannot lawfully sign anything. See the archives at http://www.gtld-mou.org/gtld-discuss/mail-archive.html.


277 See http://www.democracy.net/archive/09251997/


279 Note that “nom” is French for “name”.

280 E.g. visit http://www.iahc.org/contrib/informal.html.
example, the “Notice-97-02: Review of new generic Top Level Domains (gTLDs)”.

When will these new TLDs be available for people, commercial and non-commercial entities to register in them? First, one has to assume that the gTLD-MoU is successfully implemented and the new gTLDs are added to the root servers which make them universally accessible. Moreover, the software and technology needed must be designed and developed. To date (14 January 1998), it looks like mid March 1998, at the earliest, is a reasonable assumption. However, several people have suggested that it is possible to get a test system set up and running well within a month, and then let CORE take it over and begin running it when ready. Nonetheless, there is no urgent need for new gTLDs for another 6 - 12 months. Although “.com” is starting to get congested, several domain names in “.net” and “.org” are still obtainable.

5.2.2 Strengths and weaknesses of the gTLD-MoU proposal

The rationale behind the introduction of the new gTLDs is the massive increase in interest that the Internet is experiencing, especially

---

281 Visit the request at http://www.gtld-mou.org/docs/rfcs.html#97-02. The request for comments opened on 13 September, 1997, and concluded on 13 October, 1997. One of the discussions there was whether the TLD space “.xxx” should be established for WWW pages with “adult-oriented” content. The rationale behind the “.xxx” is that it will make it easier to isolate and filter the content from minors on the Internet. Visit the comments regarding an Internet “red-light-zone” at http://www.gtld-mou.org/notice-97-02/.

On 13 November 1997, the gTLD-MoU Policy Advisory Body (PAB) concluded a review of the seven gTLD names suggested in the gTLD-MoU. The conclusions of this review were confirmation of “.firm”, “.web”, “.info”, “.art”, “.rec” and “.nom” as names of new gTLDs and the replacement of “.store” with the gTLD “.shop”. The seven gTLDs are thus final. Shaw, R., “gTLD-MoU News” [Email - “gtld-announce”] (Received 14 November 1997). See also http://www.gtld-mou.org/docs/rfc-results.htm#97-02.

282 The software development was supposed to start on 20 October, 1997.

in the “.com” domain name space. Consequently, it has become crowded at the “.com” TLD space. As mentioned above, latecomers found that they could not obtain the domain name they wanted as a result of the “.com” being a flat name space, and accordingly disputes arose. 284 The proposal will enable entities in different fields to utilise the same domain name as SLD name, under different TLD spaces. In other words, the gTLD-MoU can amend the lack of availability of certain names. Moreover, the commercial market seems to have indicated that domain names without country codes are preferred. For instance, the natural person McDonald may hold the domain name “mcdonalds.nom”, whereas the restaurant McDonald uses “mcdonalds.com” or “mcdonalds.shop”. This is similar to the different classes of goods and services in trademark law. 285 However the current system may also provide for a similar solution for different entities with same names. The person McDonald in Norway may register the domain name “mcdonalds.priv.no”, the engineer firm McDonald in Australia can register the domain name “mcdonalds.com.au”, whereas the world-wide chain of hamburger restaurants McDonalds can register the domain name “mcdonalds.com”.

There has been suggested that the US should start using the ISO 3166 country code “.us”. 286 Consequently, each country will administer its own TLD space (i.e. the country code). Critics allege that the new TLDs further complicates trademark issues. Instead, there should be no “.com” TLD, but “.com.us” similar to Australia’s “.com.au”, UK’s “.co.uk” etc. In addition, it has been suggested that there should be only one “international” top-level domain, namely “.int” for international organisations as the UN, and define strict entrance requirements for it. As a counter-argument, this suggestion will make it harder for customers to guess and find the different

284 See Chapter 4 above.

285 See Chapter 3 above.

286 See “Table 7 - International or National Top Level Domains?” in Shaw, “Internet Domain Names: Whose Domain Is This?”, above n. 46.
commercial entities on the Internet. They would not only have to
guess the second-level domain name, but also the country code.
Furthermore, one may argue that the idea is not in conformity with
the spirit of the Internet, as cyberspace has no connections with na-
tionality and recognises no boundaries in contrast to physical space.
Users of the Internet often do not know, nor care, where in the world
the entity is situated. On the one hand, directories and Internet
search engines could amend this problem. On the other hand, if one
is trying to distinguish between several entities with the same do-
main name, the country code does not always help. For example,
there are at least three companies called “propellerheads” on the
Internet. Two are in the US and one is in Sweden. What helps more
than knowing which country the companies are situated in is that
one of them does industrial software development consulting, one
makes clothing, and one does music-related software development.
Hence “propellerheads.music” is a better identifier than
“propellerheads.se”. Moreover, several entities are world-wide in
scope, and do not want to be placed under one particular country
code. The proposal to use the “.us” is feasible in the sense that it will
solve the international administration and governance problems by
making them domestic issues. A vibrant and competitive “.us” could
also nationalise the complex trademark conflicts.

However the Internet is global in scope and inevitably one must face
the international issues it raises. Hence the gTLD-MoU recognises that some entities merit being in an “international” name
space. However, the question is whether the seven new gTLDs solve
this problem. The number of names available to specify Internet lo-
cations will increase. On the other hand, the new gTLDs overlap
with the existing “.com”. For example, a commercial entity may
register in “.com”, “.firm” and “.shop”. The effect may be confusion
for the users. However, with more TLDs the DNS will become more
similar to the real world identifiers, i.e. the identical company
names, trade names and trademarks co-existing. An expansion of the

287 Note that “.se” is the ISO 3166 country code for Sweden.
288 See Chapter 6 below.
TLD name space permitting more self-selecting categorisation can help avoid such situations as in the *Prince case* and the *Clue case*\(^{289}\) by offering the possibility for trademark owners to register in gTLDs such as “clue.games” and “prince.sports”. Hence a better solution than “.shop”, might be “.bank”, “.flowers”, “.airline” etc. and instead of “.arts”, one could have “.movie”, “.museum”, “.library” and so on.

Nevertheless, critics fear that trademark owners will attempt to register their name in several or all top-level domain spaces. Hence it will just lead to increased competition where large firms such as Coca-Cola and McDonalds will attempt to register “mcdonalds.firm”, “mcdonalds.shop” etc. in all the new gTLDs. Thus the new gTLDs will cause yet another contest between the trademark owners to register their trademarks as domain names. However this may be prevented by stricter rules for registration; for example, a requirement of a nexus between the entity’s activities and the category of gTLD.

In conclusion, the proposal of new gTLDs is desirable and feasible. There is a need for more TLDs, and perhaps more detailed categories than the seven proposed. With a proper allocation policy in a transgovernmental environment the proposal seems workable.

### 5.3 Registrars for domain names under the new gTLDs

#### 5.3.1 The CORE-MoU proposal

The seven new gTLDs will be allocated by registrars world-wide. Each registrar will become a member of the “Council of Registrars for generic Internet domain names Registrars” (CORE).\(^{290}\) The CORE is governed by two documents. The first document is called the “Articles of Association” and constitutes the articles of the

---

\(^{289}\) Hasbro, Inc. v Clue Computing, Inc., above n. 64. Hasbro owns the trademark “Clue” for one of its longest-selling and most popular board game. Clue Computing on the other hand, had registered the domain name “clue.com”.

CORE association. The second is the “Memorandum of Understanding for the Internet Council of Registrars” (CORE-MoU). The CORE-MoU is a contract entered into under Swiss law. It provides the necessary contractual, legal oversight and public policy framework under which the CORE and the individual registrars must operate.

The CORE was formed as a Swiss civil law non-profit association on 3 October 1997. Its first plenary meeting was held in Barcelona, Spain, where CORE elected an Executive Committee. Interestingly, Leni Mayo from Top Level Registries in Australia was elected Deputy-Chair and Trevor Hales from Melbourne IT was elected as a member of the committee, making Australia the only country with two representatives. The three other members of the committee are from the US, France and Germany. The second extraordinary meeting was hosted by Top Level Registries in Mel-
bourne, Australia, on 6 October 1997. CORE then started the process of reviewing the submitted Proposals for Shared Repository.297

There are two bodies which constitute the governing level above the registrars. The Policy Oversight Committee (POC) and the Policy Advisory Board (PAB). The POC is the ruling body which is advised by the PAB, and it sets policy for the CORE.298

In compliance with CORE-MoU article 4, there was an application process through which the new registrars were selected.299 The applicants had to fulfil specific requirements established by the IAHC.300 Originally, the registrars were to be allocated by lottery. However, following criticism this process was dropped.301 The registrars were originally limited to a number of twenty-eight, but as a consequence of criticism the limitation was omitted.302 Thus the number of registrars depended on the number of applications approved.303 88 registrars were approved, including Melbourne IT and Top Level Registries Pty Ltd. in Australia.304 The CORE-MoU arti-

---

297 The Shared Registry System (SRS) is the neutral, shared database repository that co-ordinates registrations from CORE registrars and causes names to enter the global Internet DNS. CORE, “The Council of Registrars”, above n. 295.

298 Connected Magazine, above n. 291. For information about the POC, see http://www.gtld-mou.org/docs/ipoc-members.html. For information about the PAB, see http://www.pab.gtld-mou.org.

299 CORE-MoU, above n. 273. The gTLD registrar application period opened on 18 July, 1997 and concluded on 16 October, 1997. Then the submitted applications were subject to approval.

300 The requirements to qualify to sign the CORE-MoU is set forth in Appendix A to the CORE-MoU. Visit the Memorandum of Understanding for the Internet Council of Registrars, above n. 273.


302 Lottery to Be Dropped from Registrar Selection Process, above n. 301.


304 View the results of the selection process at “gTLD Registrar Selection Results” [WWW - http://gtld-mou.org/docs/reg-results.html] (Ac-
5.3.2. **Strengths and weaknesses of the CORE-MoU proposal**

One important shift is that the registrars will compete directly for customers covering the same range of domain names. Thus in contrast to the current NSI system, there will be no monopoly over the new gTLDs. Section 7 (e) of the gTLD-MoU provides:

> Each CORE-gTLD Registrar may assign second level domains (SLDs) in any gTLD, described or created under the provisions of this MoU and the CORE-MoU, on a fair use, first come-first served basis.\(^{305}\)

To mediate their activities, the CORE will run a neutral, shared database repository: CORE-MoU art. 5 (f). Hence all daily activities will be handled by the registrars themselves and by CORE.\(^{306}\)

Another issue is whether the registrars should charge fees as the NSI is currently doing. The CORE-MoU article 6 (b) states, "Each Registrar may charge such fees, if any, as it determines, in its reasonable discretion, for the services it performs". In other words, it will be up to the registrar’s discretion whether a fee should be charged. Critics have argued that fees should not be charged at all. The argument is

---

\(^{305}\) See also the CORE-MoU art. 6 (a), which provides: "Each Registrar may accept applications for the assignment of SLDs in any CORE-gTLD", *above n. 273*.

\(^{306}\) Shaw, "Internet Naming Plan Signed: Additional Endorsements Scheduled For Geneva Meeting at the end of April", *above n. 265*. Donald M. Heath, chair of the IAHC, pointed out that, "With the establishment of shared registries, we have avoided monopolistic possibilities and have created a truly competitive environment". He continued, "If someone registering a name through one of the new Registrars is displeased with the service, they have the option of using other registrars".

---

cessed 10 January 1998). The site was last updated on 5 January 1998 and the list is now final.
that there should be no business interests in the granting of domain names. NSI’s practice has shown that when there is a connection between or possible impact upon the registrar’s business interests and the granting of a domain name the result may be inconsistent practice and frequent changes in the policies unfavourable to the domain name holders.\textsuperscript{307} On the other hand, since a registrar must compete on price and service and many other registrars have access to the same gTLDs, the fees are likely to mirror the market and hence be regulated by market forces.

The CORE-MoU can not dictate conditions on InterNIC or NSI. Further, it can not force the engineers that mange the root servers to add the new gTLDs to the root servers against their will. The CORE-MoU article 3 (b) provides that

Pending the expiration or appropriate amendment of the NSF Co-operative Agreement No. NCR-9218742 under which the “.com”, “.org” and “.net” gTLDs are presently administered, the “.com”, “.org” and “.net” gTLDs shall not be subject to the provisions of this CORE-MoU.\textsuperscript{308}

The plan is that “.com”, “.net” and “.org” shall be allocated by the new gTLD registrars when NSI’s contract\textsuperscript{309} expires on 31 March, 1998.\textsuperscript{310} However, to date it seems highly uncertain what will happen after the expiration. NSI has asserted ownership over the “.com”

\textsuperscript{307} Some Internet stakeholders dislike the fact that as a result of the fees charged by NSI, NSI has become a multi-million enterprise. See also Johnson, D.R., and Post, D.G., “And How Shall the Net Be Governed?” [WWW - http://www.cli.org/emdraft.html] (Accessed 22 October 1997), who purport that no statute or international convention, nor even a universal acceptance of trade practice, clearly legitimises NSI’s right to charge a fee.

\textsuperscript{308} See the CORE-MoU, above n. 273.

\textsuperscript{309} For an explanation of the NSI and its role, see Chapter 1.3.

\textsuperscript{310} Robert Shaw alleges that “Once the co-operative agreement between NSI and NSF concludes, the three existing gTLDs will be added to the shared pool”. Visit “Internet Naming Plan Signed: Additional Endorsements Scheduled For Geneva Meeting at the end of April”, above n. 265.
database. The National Science Foundation (NSF) on the other hand, has stated that they will not renew the contract after its conclusion 31 March 1998. Only time will show what the outcome of this currently evolving process will be.

5.4 Dispute resolution

As mentioned above, the domain names under the new gTLDs will be allocated on a fair use, first come-first served basis. This is similar to the current NSI policy. As discussed in detail above, the first come-first served principle has lead to disputes between domain name holders and third parties. The NSI “hands-on” approach to address these domain name disputes has been working unsatisfactorily. Hence it is important to observe that the gTLD-MoU has a different approach to this problem.

The CORE-MoU states that the registrars should not attempt to solve any disputes between domain name holders and third parties. Article 7 requires that the Administrative Domain Name Challenge Panels (ACPs) perform this duty. Further, gTLD-MoU article 8 (b) states that “Registrars shall be obligated to honour all decisions of ACPs”. Consequently, there will be no connection between the entity granting domain names and the entity solving disputes arising out of the granting of domain names. In contrast to the NSI policy, this approach moves registrars entirely out of the line of fire. This is an important alteration.


313 See the gTLD-MoU section 7 (e), above n. 263.

314 See the gTLD-MoU section 8 - Administrative Domain Name Challenge Panels, above n. 263.
5.4.1 The proposal of Administrative Domain Name Challenge Panels

The IAHC Final Report section 7 suggests that:

Administrative Domain Name Challenge Panels will be established to administer the policy that second-level domain names which are identical or closely similar to names which are, for the purposes of the Internet, internationally known, and for which demonstrable intellectual property rights exist, should only be held by, or with the authorisation of, the owners of such demonstrable intellectual property rights.115

According to the Substantive Guidelines Concerning ACPs (ACP Guidelines) section 2, any person may file a request for challenge, asking for one or more of the following forms of relief:

(1) Exclusion: that the domain name registration should be cancelled and that the SLD name may not be registered in the future by any person in the gTLD(s) mentioned in the request;

(2) Transfer: that the domain name should be transferred to the challenger; and

(3) General Exclusion: that the registration should be cancelled and the SLD name may not be registered in the future by any person in any gTLD.316

In contrast to the current NSI dispute policy, section 4 in the ACP Guidelines provides that:

if a request for challenge is lodged within 30 days of the date on which the information concerning the registration of the domain name became publicly available...ACP shall determine...whether

115 "Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs", above n. 262. The policy is implemented in the gTLD-MoU section 2 (f), see the gTLD-MoU section 8 (a), above n. 263.

In other words, the ACP will suspend the use of the domain name if a cross claim is made within 30 days of registration. Furthermore, section 6 provides that “where a request for general exclusion is lodged in the context of a challenge”, the ACP will provisionally exclude the use of the domain name during the pendency of the challenge procedure. Otherwise there will be no suspension. This is an important change from the NSI policy, where suspension is automatic on showing a prior registered trademark. Section 5 requires that the ACP consider “the relative harm that would be suffered by the domain name holder and the challenger” before making its decision to suspend the use of the domain name.

It is important to note that the gTLD-MoU suggests a policy that will still favour internationally recognised intellectual property rights similar to the NSI policy (see gTLD-MoU section 2 (f)). This begs the question whether the gTLD-MoU proposes yet another procedure that favours the trademark owners at the expense of the domain name holders. On the one hand, the gTLD-MoU recognises that a domain name holder may have protectable rights as gTLD-MoU section 2 (f) states: “Appropriate consideration shall be given to possible use of such a second-level domain name by a third party that, for the purposes of this policy, is deemed to have sufficient rights”. On the other hand, if one registers a domain name in any of the new gTLDs that embodies trademark rights owned by another person, the registration will be subject to cancellation and the SLD name excluded or transferred to the challenger if the trademark owner brings a challenge under the dispute settlement regime.

---

317 The ACP Guidelines, above n. 316.
318 See Chapter 4.2.2. above.
319 The ACP Guidelines, above n. 316.
320 Fitzgerald, above n. 272.
321 See the gTLD-MoU, above n. 263.
322 The ACPs may cancel the domain name, transfer the domain name or exclude it generally: ACP Guidelines section IV B 7. Note also that the
Thus a domain name holder with no trademark rights to the domain name might still be without protection.

The ACPs shall make their determinations upon balancing all the circumstances of the case. Similar to the NSI policy, common law intellectual property rights may not be deemed as sufficient evidence of the existence of an intellectual property right. In contrast, evidence of widespread public recognition of the domain name holder’s use is one factor the ACPs must consider. Moreover, there is suggested an important change in the ACP Guidelines section IV C 21: if the domain name has been used for two years, the domain name holder’s rights will be given more consideration. Then there will be a presumption in favour of the domain name holder. This is an improvement compared to the NSI policy.

ACPs may suggest modifications in the SLD name to avoid conflict with the rights of the challenger, above n. 316.

See the ACP Guidelines, section IV C. The first come-first served principle, intellectual property rights of the challenger, rights and interests of the domain name holder, whether either party has acted in bad faith, the similarity between the SLD name and the alphanumeric string that is the subject of the intellectual property right, the use being made of the domain name and potential impact on the parties and any third parties shall be considered, above n. 316.

See the ACP Guidelines, section IV C 15, above n. 316.

See the ACP Guidelines, section IV C 20, above n. 316.

The ACP Guidelines section IV C 21 states: “A finding by the ACP that the domain name has been used by the domain name holder continuously and in good faith on the Internet for two years prior to the date of lodging of the challenge shall give rise to a rebuttable presumption that the domain name holder is entitled to continue that use of the domain name”, above n. 316.

Nevertheless, Brian Fitzgerald argues that “One outstanding problem still is that the NSI dispute policy and the gTLD-MoU is premised on the notion that any one trademark owner has a clear priority to a specific domain name over the other trademark owners from different countries and in respect of different goods and services”. Fitzgerald, above n. 272.
Critics have argued that as a result of the dispute resolution policy the holder of a SLD in one gTLD (e.g. “springwater.com”) may be able to assert some right to the identical SLD under another gTLD (e.g. “springwater.firm”). On one hand, the mere fact that one holds a domain name under one gTLD can not lead to any rights in the identical SLD under another gTLD. One of the reasons for adopting additional gTLDs was to allow others to use some of the “good” names in the new gTLDs. However, if you do business under a SLD and the domain name has become associated with the source of supply of your goods or services; for example, “Coke”, you may be entitled to lay claim as the intellectual property owner of this string as your trade or service mark and to use it in any other gTLD. In other words, one can pursue an ACP challenge, and if successful, one may be able to deny the SLD to anyone else in any other gTLD.

5.4.2 Should the dispute resolution be left to the courts?

As mentioned earlier, the various domain name policies provide different approaches to the domain name dispute settlements. The most satisfactory seems to be the “hands-off” approach. In connection with the new gTLD-MoU approach to domain name disputes, it is important to address the question whether domain name disputes should be left to the courts.

The gTLD-MoU section 8 (c) provides:

No decision of an ACP shall inhibit, affect or prevent the power of the appropriate national or regional courts to hear cases interpreting and enforcing intellectual property rights that fall within their jurisdiction. Likewise, nothing in this Section shall prevent any party,

328 gTLD-MoU Frequently Asked Questions, above n. 276. The FAQ states that “if you are first in line, you can obtain the domain names that you want in the new gTLDs, even if they are already registered by someone else in .com”.

at any time, from bringing any case before such national or regional courts that could otherwise be brought, nor from initiating arbitration or mediation procedures that are otherwise available.\textsuperscript{330}

Is there any necessity for alternative procedures for domain name disputes? On one hand, recognizing the increase of commercial activity on the Internet a means for dealing with conflicts between domain names and intellectual property rights is required. One may argue that with the globalisation of domain name registrations, the dispute resolution system should somehow have to be international or global in nature.\textsuperscript{331} On the other hand, one part of the present system of TLDs has a distinctly national character; the country code TLDs are clearly national in character. Hence disputes involving domain names in the country code TLDs seem to have a national forum for dispute settlement: the dispute can reasonably be brought to a court in the country which the TLD is related to.

However, it is not clear how decisions of a single national or regional court can be implemented in the context of a global domain name registration system. For example, a court of the country where one registrar is located issues an injunction against registration of a SLD name. Then the losing party just goes to a registrar in another country where the injunction would have no effect, and re-registers the same domain name. Similarly, whether or not one fails in an ACP challenge, one may exercise all the rights of an intellectual property owner by seeking court action in any nation to demand "cease and desist" use of one's intellectual property and seizure of the trade or service mark and all related "goodwill" which goes with it. In theory, the new ACP system provides for direct implementation of the results of the dispute resolution. The ACP awards will be enforced with global effect. One single procedure for all gTLDs is a

\textsuperscript{330} The gTLD-MoU, above n. 263.

\textsuperscript{331} WIPO, "Resolution of Intellectual Property Disputes within the context of the Memorandum of Understanding on the generic Top-Level Domain Name space of the Internet Domain Name System (gTLD-MoU)" [WWW - http://www.wipo.org/eng/Internet/domains/tdn/cm/cm_i_3.htm] (Accessed 22 July 1997).
preferable solution. However, in practice, how can a decision be enforced with lacking national judicial authority?

The proposed gTLDs are not country-related, and they will be granted by registrars located in different countries. Thus the new gTLDs have no country affiliation. Does this mean that what is required is an international dispute settlement system that is not affiliated with any one country, or the laws of any country, to accommodate what is becoming a global system? On one hand, it must be recognised that there is no global intellectual property law and no established global forum for adjudicating intellectual property disputes. On the other hand, international law needs to “catch up” to the needs of commerce on the Internet, and some alternative form of dispute resolution is needed to temporarily “fill the gap”. The ACPs may be said to temporarily fill this gap. As the national courts may face conflict of laws problems when trying to solve cross-border disputes, submitting a dispute to international arbitration may solve the problem. Nevertheless, this paper will argue that the ACPs will face difficulties regarding enforcement and compliance as a result of the incomplete national and international judicial authority.

5.5 The opposition against the gTLD-MoU

Not surprisingly, NSI leads the opposition to the gTLD-MoU. Another equally critical, independent effort against the gTLD-MoU is

332 The development of cross-border disputes, such as the Prince case, has highlighted that this single procedure should be an international arbitration. As mentioned, one of the problems with the NSI dispute resolution policy is that it provides the trademark owner with two options. She can invoke the NSI policy or go to the courts. In the Prince case, although the plaintiff secured a declaration under s.21 of the UK Trade Marks Act 1994, the opportunity was open to the defendant to return to the US - where the domain was registered - and attempt to invoke NSI’s dispute resolution policy or commence an action there. This raises the spectre of anti-suit injunctions, cross-border litigation or cumbersome enforcement of foreign judgements. Thus, the case is a poignant reminder of the potential pitfalls in cross-border trade mark disputes over domain names, above n. 204.
the Stop-gTLD-MoU web site. Also, there is interesting material among the 425 responses in the Comments on the Registration and Administration of Internet Domain Names. This section will provide an overview of some of the objections.

The major areas of objections to the gTLD-MoU are: no authority, sweeping powers, inadequate public input, uncertainty over NSI's post co-operative agreement status, increased root server traffic, double taxation, Swiss jurisdiction, limited TLDs and customer confusion. Moreover, critics have alleged that some of the approved registrars engage in the practice of reselling domain names. Hence they feel that there is a conflict of interest.

5.5.1 The NSI opposes the gTLD-MoU proposal

NSI posted a response on April 29, 1997, "Secure Internet Administration and Competition in Domain Naming Services" [WWW - http://www.netsol.com/papers/Internet.html] (Accessed 15 October, 1997), where it opposes the gTLD-MoU and proposes another approach for secure administration of the key functions of the Internet. In "What They Are Saying About the IAHC Plan" [WWW - http://www.netsol.com/announcements/quotes.html] (Accessed 15 October, 1997), the NSI has created a WWW site with citations of important persons saying that they are concerned about the gTLD plan. For example: "We are concerned about numerous aspects of their plan, Clinton administration official".


Visit the comments site at http://www.ntia.doc.gov/ntiahomedomainname/email. This is the home of responses to the US Department of Commerce's Notice of Inquiry (NOI) into the Administration and Registration of Domain Names. The NOI was open from 1 July through 18 August, 1997.

See also Tebbe, M., "Heads up! Internet domain names will be getting goofier" (1997) 19 (8) InfoWorld 62 at 62.
The NSI alleges that the proposal “risks the fragile stability of the Internet”.\(^{337}\) It believes that the proposal is too complex to succeed and that the approach is too bureaucratic. Moreover, the NSI assesses the proposal to be too narrow in the sense that it does not address the total situation. The NSI argues that the proposed approach to domain name disputes appears unworkable and will create increased conflicts. Further, the NSI says that “simultaneous registration of domain names by multiple global registrars will create a global litigation nightmare”.\(^ {338}\)

Another problem with the gTLD-MoU is the legitimacy of the IAHC. The NSI criticises the IAHC for holding “no legal authority”. Several critics have questioned where the organisation acquired its authority.\(^ {339}\) It has been criticised because the IAHC has no US congressional mandate to impose regulation, levy taxes, allocate namespace, grant lucrative contracts, or collect license fees.\(^ {340}\) On the other hand, one may argue that IAHC acquired its authority from “rough consensus”. In defence of the gTLD-MoU approach, the In-

---

337 “Secure Internet Administration and Competition in Domain Naming Services”, above n. 333.

338 The NSI argues that “while detailed in its discussion of a small subset of the hundreds of currently existing TLDs, the IAHC proposal remains silent on the three truly critical functions of the Internet administration: the allocation of IP addresses, the management of Internet identifiers, and the administration of the “dot” (the root of the TLD structure and the global servers that support it)”. “Secure Internet Administration and Competition in Domain Naming Services”, above n. 333.


340 Ellen Rony, “gTLD-MoU questions” [Email] (Received 14 October 1997). She alleged that even an informal White House task force, chaired by the US Office of Management of Budget, is concerned about the use of United Nations’ intergovernmental bodies (WIPO and ITU) to implement a plan when member organisations had not provided input. She informed me that the White House will release guidelines that say international Internet regulation could devastate the commercial potential of the nascent network.
ternational Bureau of WIPO has stated that “it [the gTLD-MoU] represents a compromise solution, adopted by rough consensus in the context of the gTLD-MoU, for dealing with trademark-SLD conflicts”.  

The NSI purports that the “problem of domain name disputes on the global Internet cannot be adequately resolved by an arbitration body lacking international or at least national judicial authority. The dispute problem requires a body of international law, or at least civil procedure, that is specifically applicable to domain names and trademarks”.  

In conclusion, the critique of the gTLD-MoU must be seriously considered. Several Internet stakeholders see tremendous problems with the proposal. It is clear that the gTLD-MoU is not perfect. However, there are also several Internet stakeholders that believe the proposal is a good idea, or at least a good start. One thing is certain, the gTLD-MoU is an attempt to address important Internet issues and presently there are no other attempts that examine the issues more thoroughly.

5.5.2 Advantages and disadvantages of the gTLD-MoU

In summary, the advantages of the gTLD-MoU are that it avoids monopolistic practices and provides new gTLDs - which are likely to dilute the popular “.com”. The gTLD-MoU removes the registries from the domain name dispute resolution and provides an independent and international dispute resolution body. Further, the gTLD-MoU brings together private entities and organisations, international and national, and provides a system of Internet governance at the international level. The gTLD-MoU assures the domain name holder


stronger rights - hence it attempts to balance the rights between domain name holders and trademark owners.

The disadvantages of the gTLD-MoU are that trademark owners might attempt to register their trade name in all the new gTLDs - which may lead to another domain name competition between companies and other entities. In addition, it is uncertain whether the gTLD-MoU will be implemented and complied with by the whole Internet community. Finally, and perhaps most importantly, it is unclear how decisions made by the ACPs may be implemented, enforced and complied with. The dispute resolution body lacks judicial authority, thus the parties may still go to their national courts - thus multi-jurisdictional and cross-border litigation problems are still present.
Aims of chapter 6

The aims of Chapter 6 are to:

* outline the problems the transnational Internet creates for the current domestic legal systems;

* analyse whether there should be self-regulation of the Internet, state regulation, or international governance by international organisations; and

* critically evaluate the proposed models for Internet governance, analyse the gTLD-MoU as a case study and propose a solution.

The current domain name system, as described in detail in the previous sections of this paper, is coming to an end on 31 March 1998. The co-operative agreement between NSI and the NSF then expires. At present, although there are proposed changes in the gTLD-MoU and CORE-MoU, there is no universally agreed replacement. Without a domain name system, the Internet will come to a halt and there will be chaos regarding where and how one can register a domain name. This chapter argues that what we urgently need, is an agreed system of governance that is truly representative, responsible and accountable. Until now, there has been no law and order in cyberspace. Our current national legal framework is designed for a world of barriers and distance. However, the Internet transcends

---

Rony, E., “Registration and Administration of Internet Domain Names”, above n. 311.
national boundaries and limits. The Internet is truly global and no one country can control it any more than they can control the sea or air.\textsuperscript{344} Thus current domestic law does not adequately resolve the problems the Internet poses.\textsuperscript{345} In order to maintain public confidence in any system of domain name allocation, and thus provide a secure environment for the commercial activity on the Internet, a formal legal and public policy framework is required. This will reduce the need for litigation of the type witnessed recently.

6.1 The Internet creates problems for the current domestic legal systems

Before narrowing the scope to a discussion of Internet governance and whether there should be self-regulation or international governance, it is important to have an understanding on how domestic legal systems and the Internet intersect.

The Internet is transnational, borderless and multi-jurisdictional. The world-wide network of computers is not within the territorial jurisdiction of any sovereign nor subject to rules centrally laid down.\textsuperscript{346}

\textsuperscript{344} Frank, \textit{above n. 22} at 17.

\textsuperscript{345} Selin, S., "Governing Cyberspace: The Need for an International Solution" (1996/97) 32 \textit{Gonzaga Law Review} 365 at 372. Selin explains that "Traditionally, nations have asserted sovereignty and law based upon national borders and their coercive power. There are few international "rights", because international treaties typically establish coordinated, national standards instead of a single, unique global right. Formerly, treaties and national boundaries have provided an adequate way of dealing with international problems". His point is, however, that the Internet "tends to ignore national boundaries and previous treaties have not adequately envisioned this medium". See Selin at 379 and 380.

Thus “national borders are just speedbumps on the information superhighway”. The Internet challenges our current domestic law. It raises questions about territoriality, authority and sovereignty in cyberspace. Moreover, there are questions about bottom-up or top-down methods of achieving law, and about sovereignty and its connection to territory.

One of the first problems domestic legal systems face when confronted with the Internet, is the enforcement and compliance problem. If one country passes legislation aimed at managing and controlling the Internet, there is only modest enforcement powers on non-citizens that operate on the Internet. Even if an international treaty were developed that most of the industrialised countries agreed to, how would one enforce the provisions to a non-participant to the treaty? Some governments have tried to enforce control over the Internet, but the efforts have been directed to the portion under their immediate authority. Other governments have resigned themselves to the fact that the Internet is multi-jurisdictional and thus accepted that rules can not be enforced by one single government on a Internet-wide basis.

This leads to another problem domestic legal systems have experienced when endeavouring to deal with Internet activities. The Internet causes problems with jurisdiction and other related criminal law problems. For example, will mere accessibility of a WWW site in a

347 Quoted in Selin, above n. 345 at 366.
348 Radin, and Wagner, above n. 346.
349 Selin, above n. 345 at 370.
350 Selin has one example that shows how difficult it is for individual governments to exercise jurisdiction over its people when the Internet is involved. The French government had banned a book about the late president Francois Mitterand. However, before the authorities were able to stop sales of the book, it was uploaded onto the Internet by using host computers in France and in other countries. France does not have the jurisdiction to ban the book from servers located in other countries, hence it is powerless to stop its distribution. Furthermore, France can not reasonably prevent its citizens from downloading and reading the book. See Selin, above n. 345 at 372.
territory be sufficient to establish jurisdiction in that territory over
the entity which owns the WWW site? Activities taking place on
the Internet can sometimes result in a tri-jurisdictional dispute. The
country where the information was transmitted, the country
where the Internet service provider is located, and the country where
the transmission is accessed, may all be involved in the dispute.

Flint argues that The Playboy Enterprises Inc. v Chuckleberry Pub-
lishing Inc., CompuServe Inc. v Patterson, Maritz Inc. v Cybergold
and Inset Systems Inc. v Instruction Set Inc., suggest so. On the
other hand, in Bensusan Restaurant Corp. v King, 1996 WL 509716
(S.D.NY Sept. 9, 1996) the court decided that the mere fact that an
Internet site was accessible in New York did not mean that, in the ab-
sence of anything else, the site was directed to persons in New York
such as to give the courts of New York jurisdiction. Flint, above n. 255
at 165. See also “Current Developments” “No Personal Jurisdiction
Lawyer 24 at 24.

There is a list of cases that discusses the propriety of a court’s exercise
of personal jurisdiction over defendants based upon the defendant’s
Internet activities, available online. See Post, D., “Personal Jurisdic-
tion on the Internet” [WWW - http://www.cli.org/DPost/jcases.html]
(Accessed 22 October 1997). The reason why the American theorists
divide the jurisdiction into personal jurisdiction and subject-matter ju-
risdiction, is that subject-matter jurisdiction refers to a court’s power to
decide the particular dispute at hand. For example, only federal courts
have subject-matter jurisdiction over copyright and patent cases,
whereas only a state court has subject-matter jurisdiction over contract
cases between citizens of its state. The rules for subject-matter juris-
diction are rarely disputed. Personal jurisdiction, however, is more
complex. Personal jurisdiction is the power to make the wrongdoer
obey its orders. Smedinghoff, above n. 93 at 365. See also Rosenoer,
above n. 1 at 227.

Selin, above n. 345 at 371.

Note that the Internet service providers (ISPs) are neither administra-
tors nor managers of the Internet. The ISPs simply provide access to
the Internet. Several countries have attempted to hold the ISPs liable
for illegal information obtained on the Internet through the providers.
However, as Selin points out, this is a mistake “like someone would
blame AT&T for an obscene call or a local broadcaster for a network
program they have watched”. Selin, above n. 345 at 374.
Due to the transnational nature of the Internet, in many cases there will not be the relevant nexus with the state (e.g., Australia) in which the trademark holder can sue. If an alleged breach occurs on the Internet and all that connects that breach to Australia is a passive WWW site, then it is doubtful whether exorbitant jurisdiction would be exercised by the courts.354 Indeed, the US courts have already found it difficult to identify what creates a sufficient nexus to give jurisdiction.355

354 See O11r1(2) Supreme Court of Qld Act 1991.

355 For example, Hearst Corp v Goldberger (1997 WL 97097 (S.D.N.Y., February 26, 1997)). In that case, the court found that mere ownership of a WWW site that is accessible to, and visited by, New York computer users does not constitute sufficient contacts with the state of New York to provide New York courts with personal jurisdiction over the WWW site owner. See “Current Developments” “Web Site Does Not, By Itself, Give New York Court Personal Jurisdiction” (1997) 14 (4) The Computer Lawyer 28 at 28. In Zippo Manuf’g Co. v Zippo Dot Com, Inc., 1997 WL 37657 (W.D. Penn. Jan. 16, 1997) [WWW http://www.bna.com/e-law/cases/zippo.html] (Accessed 2 November 1997), the court ruled that the WWW site of a company in California was sufficient to give the court in Pennsylvania jurisdiction over a trademark dispute brought by a Pennsylvania company. See “Current Developments” “Interactive Web Site Is Sufficient for Jurisdiction, District Court Rules” (1997) 14 (3) The Computer Lawyer 32 at 32.

Theoretically, a country could claim jurisdiction over an individual’s Internet activities, regardless of where that individual is located. The country could use the “territoriality principle”, and regard the activity as taking place within their territory. Selin, above n. 345 at 371. Moreover, Selin argues that the “double criminality” principle is necessary to the successful operation of international criminality law. Selin, above n. 345 at 387. Post purports that because sysops must have physical hard disks that are present within particular territorial areas, they are clearly subject to the jurisdiction of the countries where they conduct their operations. For example, the US could pass a law threatening to shut down the operations of all sysops within its reach that do not abide by specific rules. Post says that if such a bill were to pass, substantial compliance by US-based systems would surely follow. Johnson and Post, “And How Shall the Net Be Governed?”, above n. 307.
Other problems for domestic legal authorities on the Internet are issues such as the lack of standards for evidence collection, the problem with the wide use of anonymous remailers, censorship, and human rights issues. These issues will not be addressed in this paper.

6.2 The proposed models for Internet governance: self-regulation or international governance?

As the Internet is a global system, it is hard to comprehend how any set of policies, procedures or rules will perfectly work under every situation. As seen, there are several pitfalls in cross-border trademark disputes over domain names. The domestic legal systems face problems when attempting to deal with online activity. The Internet weakens many of the traditional institutions for governance. No one has an uncontested or clearly legitimate claim to authority to set Internet policy matters unilaterally. From this it might be said that international law should govern the Internet. This section will critically evaluate the models for Internet governance and analyse whether a system of self-regulation provides a satisfactory management of the Internet, whether the gTLD-MoU is the most feasible solution or whether the Internet would merit from a system of transgovernmental governance.

Currently, there are four basic competing models for governance of the Internet:

* Territory-based law. Existing territorial sovereigns may seek to extend their jurisdiction to govern actions on the Internet that have substantial impacts on their own citizenry;

* International treaties. Sovereigns may enter into multilateral international agreements to establish uniform rules applicable to conduct on the Internet;

356 Selin, *above n. 345* at 370.

357 Johnson and Post, “And How Shall the Net Be Governed?” *above n. 307*.

358 See Chapter 6.1. *above*. 
* Decentralised self-governance. *De facto* rules may emerge as a result of the complex interplay of individual decisions by domain name and IP address registries, system operators and Internet users; and

* International organisations. A new or existing international organisation may establish rules to govern the Internet.

As the Internet is a global, border-disregarding place, individual attempts at regulating this world-wide system seem futile. Most attempts to define new rules rely on the disintegrating concept of territory and thus ignore that the new network and technology transcend national boundaries. Due to the lack of national borders on the Internet, one may ask if an adequate way for countries to assert any control over the Internet involves the initiation of an international dialogue, creation of an international understanding, or the negotiation of an international agreement governing this new medium. For example, the existing international principle of *jus cogens* could possibly be used as a basis for regulating speech content on the Internet. *Jus cogens* mandates that certain forms of behaviour are unequivocally intolerable.

Traditional treaty practice rests on a dualist approach to the relationship between international and state law. The dualist theory considers international law and municipal law to be two separate legal orders operating and existing independently of one another. Neither system has the power to neither create nor alter the rules of the other. A solution for Internet governance that could be workable is

359 Selin, *above n. 345* at 366. As seen above, in Chapter 6.1., state governance of the Internet is not feasible.

360 See Selin, *above n. 345* at 384. He states that “Advocates suggest that speech which incites behaviour condemned by the *jus cogens* principles could be regulated”. However, *jus cogens* is not sufficient. Selin argues that while *jus cogens* might form the basis of some international norms which could be applied on the Internet, there is need for an international agreement that requires more guidance than *jus cogens* can provide. See Selin at 385.
an international agreement on domain names.\textsuperscript{361} However, it is not clear how any treaty or international agreement could obtain agreement from all nations. David G. Post notes that no treaty regime is likely to succeed in imposing any uniform rules on the Internet unless every sovereign whose citizens connect to the Internet joined in the agreement.\textsuperscript{362} Any authority will only be globally authoritative if its decrees are accepted by every national sovereign. However, this would, according to international law theorist Margaret Jane Radin, require a full-scale network of treaties.\textsuperscript{363} One could also imagine a piecemeal process of treaty-making, issue by issue. However, as

\begin{footnotes}
\item[361] For example, a solution that could be workable is an international agreement on domain names similar to what the Berne convention does to copyright. (In December 1996, international copyright treaties were signed in Geneva. The treaties were created to address copyright protection for digital intellectual property. Treaty I protects digital literature and artistic work under current international law. Treaty II applies copyright protection to digital music or sounds. Treaty III, dubbed the sui generis database treaty, was abandoned. Macavinta, C., "Geneva treaty wins over sceptics" [WWW - http://www.news.com/News/Item/-0,4,6437,00.html] (Accessed 6 November 1997)). Each country could then formulate its own local laws based on this. In this sense, the body of intellectual law has over time been expanded from patent, copyright and trademark to patent, copyright, trademark and domain name law. This would be a more traditional international approach. On the other hand, Post states that the treaty process is too slow, especially in contrast to the extremely rapid development of new technologies on the Internet. Moreover, if one agreed upon some core principles for the governance of the Internet in a treaty, such an agreement would take the form of a high level document with a fair degree of generality, Post argues. However, the Internet continuously presents novel questions that test our prior understandings of law. See Johnson, D.R. and Post, D.G., "And how Shall the Net Be Governed?", \textit{above n. 307}.

\item[362] Johnson and Post, "And How Shall the Net Be Governed?" \textit{above n. 307}. Moreover, Post purports that the negative externalities created by actions sanctioned in countries that do not agree with the majority, are likely to be substantial.

\item[363] Radin, \textit{above n. 346}. See also Johnson and Post, \textit{above n. 307}, who argue that the very difficult task to get every sovereign to join in the agreement, suggests that the treaty route to Internet governance is unlikely to be successful.
\end{footnotes}
Slaughter points out, this kind of world government, even as an ideal, is unfeasible at best and dangerous at worst.\textsuperscript{364} She exemplifies this with the UN. The UN “cannot function effectively independently of the will of the major powers that comprise it; those powers, in turn, will not cede their power and sovereignty to an international institution”.\textsuperscript{365} This paper will argue that the traditional reluctance to cede sovereignty to international institutions would cause problems when attempting to create Internet governance through an international agreement.

Self-regulation is seen by several Internet users as an attractive possibility, primarily because it is seen as offering a realm of free choice.\textsuperscript{366} Internet users would like to consider the Internet as its own \textit{sui generis} jurisdiction, with its own self-governance and enforcement mechanisms. Until now, the technical organisations, such as the IETF, have in effect created a complex adaptive system that produces a type of order that does not rely on lawyers, courts, statutes or votes.\textsuperscript{367} Given the apparent difficulties of using top-down processes to accomplish unterritorialisation, many of those who are interested in the Internet are thinking about self-governance rather

\textsuperscript{364} Slaughter, \textit{above} n. 269 at 1.

\textsuperscript{365} \textit{Ibid}

\textsuperscript{366} Freedom of expression is the key to growth of the Internet. There is a basic right to communicate, beyond the right to receive information as recorded in the Universal Declaration of Human Rights. Selin, \textit{above} n. 345 at 378. See Tarjanne, P. “The ITU Responds to New Concepts for Public Policy in the Global Information Society” (1992) 13 \textit{Intermedia}. The Secretary-General of the International Telecommunication Union, Pekka Johannes Tarjanne, proposed seeking the insertion of a “right to telecommunicate” into the Universal Declaration of Human Rights.

\textsuperscript{367} Johnson and Post, “And How Shall the Net Be Governed?”, \textit{above} n. 307. The basic philosophy of the Internet can be described by the IETF motto: “We reject Kings, Presidents, and Voting: We believe in rough consensus and running code”.

124
than planning. In other words, they are thinking about a regulation which is not laid down, but grown up.\textsuperscript{368}

An American professor, David G. Post, has argued that self-governance of the Internet is desirable. According to Post, a network of contracts among the participants on the Internet may substitute for external regulation. He argues that the same decentralised decision-making that created the Internet and currently runs the Internet at the structural level (e.g. the technical protocols) can be applied to governance of the Internet at the substantial level.\textsuperscript{369} Post also suggests that the enforcement mechanisms could be laid down by the “sysops”.\textsuperscript{370} Internet users could then contract freely to move easily among online spaces thereby voting for the rules and environments they prefer. The rationale behind this proposal is that the sysops would hold the ultimate power - banishment.\textsuperscript{371} Moreover, Post suggests that the domain name registration authorities should “co-ordinate to condition domain name use by sysops on certain basic prohibitions of fraud and force”.\textsuperscript{372} In other words, Post suggests that the Internet should continue its informal system of self-

\textsuperscript{368} Radin, \textit{above n. 346}.

\textsuperscript{369} Post notes that the rules at the technical level evolved from the decentralised decisions by individuals to adopt a promising standard because it served their own interests. See Johnson and Post, “And How Shall the Net Be Governed?”, \textit{above n. 307}.

\textsuperscript{370} Johnson, D.R., and Post, D.G., “And How Shall the Net Be Governed?”, \textit{above n. 307}. The “sysops” are defined as “the system operators, who control ID issuance and the servers that hold files”. In other words, the sysops of the Internet are the engineers that manage the root servers, the registries that allocate domain names, the Internet service providers that provide Internet access etc.

\textsuperscript{371} Technically, it is possible to “pull the plug” and exclude someone from the Internet. For example, the Internet Service Providers (ISPs) can withdraw your IP address. Without an IP number, you will not have an Internet presence.

\textsuperscript{372} Johnson, D.R., and Post, D.G., “And How Shall the Net Be Governed?”, \textit{above n. 307}.
However, one may argue that one should clearly distinguish between the two parts of the Internet system: the structure and the substance. One may debate whether Post is confusing the technical system (i.e. the structure) of the sysops with governance (i.e. the substance). A decentralised process adopted in regard to transmission protocols can be unambiguous because a packet either has TCP/IP headers or it does not, and a document either complies with HTML standards or it does not. Rules regarding “fraud” and “infringement”, on the other hand, can not be identified as easily.

In essence, Post proposes that the sysops and the domain name registries should substitute for state institutions as the key players in Internet governance. A counter-argument is, however, that sysops may standardise on onerous “take-it-or-leave-it” terms under the threat of exclusion. Radin criticises Post’s views and draws the analogy of residential private government. Systems of private covenants, in subdivisions or condominiums, have been praised as a method of choice-based community creation. Sysops terms and con-

---

373 It is not clear that decentralised contractual law-making on the Internet for enforcement purposes would result in the desired ends of diversity and choice. As mentioned above, the sysops of the Internet, currently use RFCs. These Internet organisations are for-profit commercial entities. Hence fiscal concerns might be a factor in the establishment of policies. Radin, above n. 346.

374 The structure consists of the technical system with IP addresses, RFCs, root servers and Internet Service Providers (ISPs). The substance consists of the domain names, the allocation and registration of domain names and the domain name dispute policies.

375 Post’s argument may be said to be “old-fashion”. Up until now, the technical people has been running the Internet. The trend is, however, that the commercial sector takes over the substance of the Internet and leaves the structure to the technical entities. There will be mechanisms so the power will not maintain with the technical part of the Internet, but will be vested in the organisations which manage the substantial part of the Internet.

376 This is the opposite of what Anne-Marie Slaughter suggests, see Slaughter, above n. 269 at 6.

377 Radin, above n. 346.
ditions have also been criticised because they are imposed on would-be residents on a "take-it-or-leave-it" basis.\textsuperscript{378} Another counter-argument is that those who are banished from the Internet will resort to the courts, either in their own countries or in the country in which the registration authority is located. Hence it is almost unavoidable that national courts will interfere with the domain name disputes. Radin suspects that with Post's proposal the enforcement mechanisms will evolve on the Internet into a "hybrid of internal self-regulation and external sovereignty". As a solution, Radin suggests that the national courts could develop a kind of comity between the Internet and the territorialised non-virtual world, abstaining from Internet disputes in favour of the Internet's own processes.\textsuperscript{379} If cyberspace acquired its own sovereignty "perhaps other sovereignties would not question its authority to de-nationalise (banish) its citizens. But perhaps it's more likely that such an eventuality would cause the world's sovereigns not to recognise any sovereign's general right to de-nationalise its citizens, at least where denationalisation would deny the ability to engage in meaningful commerce".\textsuperscript{380} This paper will argue that self-governance is not the most efficient, workable and feasible solution for Internet governance.

This leads to the question whether the Internet would merit from international governance. In contrast to an international treaty, an in-

\textsuperscript{378} Ibid

\textsuperscript{379} See also Johnson and Post, "And How Shall the Net Be Governed?", above n. 307. Post argues that sovereigns should defer action and see whether the collective actions of domain name registries and sysops produce a set of operational rules that provides reasonable protection for the vital interests they are charged to protect. On this background, Post also suggests that an international organisation for Internet policy making should not be created until it has been demonstrated that less formal mechanisms will not work.

\textsuperscript{380} Radin, above n. 346. As a comment to Radin's last point, it may be said that exclusion from the Internet, the tremendous vehicle for commercial transactions and advertising, may be a too hash reaction. A system of governance of the Internet should address the serious problems in connection with online activity only, and not become to regulation-bound.
ternational organisation does not need to obtain the agreement of all interested governments. Hence an international organisation may attempt to establish and enforce basic rules for the Internet. Until now, the Internet has been created and run by voluntary, private persons and entities. The gTLD-MoU is an example of international

381 See Johnson and Post, “And How Shall the Net Be Governed?” above n. 307.

382 The US Government once claimed that the US Department of Defense (DOD), operating through the FNC, “owns” the domain name space. This was a controversial claim. It is correct that the US government, through NSF and DOD contracts, has had a strong hand in guiding DNS policy. As mentioned above, the Internet has its origin in the US. However, as the Internet is a global system of interconnected computer networks, the US, or any one country, cannot own the domain name space. There is no contract, constitution or treaty that gives the US Government the right to set policy regarding domain names. See Johnson, D.R. and Post, D.G., “And How Shall the Net Be Governed?”, above n. 307. The US government has now supported the transition to the private sector and one interesting development is the US Department of Commerce’s “Inquiry into the Registration and Administration of Domain Names”. Visit http://www.ntia.gov/ntiahome/domainname/domainname.htm, which reads in part; “The Government has supported the privatisation and commercialisation of the Internet through actions such as the transition from the NSFNET backbone to commercial backbones. The Government supports continued private sector leadership for the Internet and believes that the transition to private sector should continue”. Nevertheless, a significant amount of people in the US feel that the Internet is US “property”. They do not like the “Geneva-proposal” (i.e. the gTLD-MoU), and several discussions regarding this topic have occurred on the various mailing lists. On the other hand, the US is “allergic” against monopolies. Hence they do not like the NSI regime. The majority of the US people on the mailing lists want a change, the problem is - a change to what?

The EU and its member states have indicated their interest in having further opportunity to hear others’ views and make their views known. Stoodley, above n. 23 at 514. Selin, above n. 345 at 386 informs that in April, the EU ministers asked their Commission to determine whether the EU should deal with the issue, or whether the issue should proceed directly to international negotiations.
organisations providing an international Internet governance institution with authority to lay down rules about domain names.\textsuperscript{383}

6.2.1 International organisations

As the Internet is a global resource the allocation of domain names is a global issue. The gTLD-MoU s 2 provides that the TLD name space “is a public resource and is subject to the public trust”. Furthermore, domain name allocation “is a public policy issue” and allocation must be in the best “interests and service of the public”.\textsuperscript{384} The world-wide scope, and the lack of geographic boundaries and limitations, makes the Internet well suited to be administered and governed by international organisations.

One counter-argument, however, is whether an international organisation is representative of all the Internet stakeholders. For example, WIPO, who will implement the gTLD-MoU proposal, is an interna-

\textsuperscript{383} Currently, it is not clear who has the ultimate authority to grant and revoke a domain name. For example, it would be interesting to examine where the IANA, who has played an important role in the stability of the Internet, gets its authority from. For information about the IANA and its role, see Part I, Chapter 1.3. “The main Internet players” above. According to the IANA web page, the IANA “is chartered by the Internet Society and the Federal Network Council”. Visit IANA Overview at http://www.isi.edu/iana/overview.html (Accessed 8 November 1997). Hence the next question is, where did the Internet Society and the Federal Network Council (FNC) get their authority from? The FNC is chartered by National Science and Technology Council’s Committee on Information and Communications (CIC). See Federal Networking Council Charter at http://www.fnc.gov/FNC_charter.html (Accessed 8 November 1997). This appears to be the end of an authority trail, since the CIC is one committee of a US “cabinet-level council [which] is the principal means for the President to co-ordinate science, space, and technology policies across the Federal government”. See National Science and Technology Council Committees and Subcommittees at gopher://cyfer.esusda.gov:70/00/ace/nstc/nstc-comm/committee. Also see http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html. This is just one example of the complicated network of authorities involved in the Internet governance and administration.

\textsuperscript{384} The gTLD-MoU, above n. 263.
tional organisation for intellectual property. Hence it has been questioned whether WIPO is representative of the users of the Internet. The nexus between intellectual property rights and the governance of the Internet is not obvious. Critics also ask whether WIPO, being situated in Geneva, Switzerland, represents European, American, Asian and Australian interests equally. Moreover, who should be represented given a world in which the notion of separate "individuals" is virtually meaningless? Another problem with a world-wide organisation is how to protect the basic rights of minorities.

Another obstacle is how a non-governmental organisation can impose its rules on the Internet as a whole. This is the primary problem of the gTLD-MoU proposal of ACPs. Further, even if an organisation controlled the current DNS, how could it prevent the creation of a new one? And by what right would an international organisation govern the Internet? Corruption could also occur.

On the other hand, the gTLD-MoU proposal's strongest asset is the numerous international organisations and entities which are signatories to it. The endorsements of the MoU by a significant number of entities around the world give it authority and a global acknowledgement that the Internet community wants the change. The considerable number of signatories makes the gTLD-MoU representative. Hence it might gain a reputation and authority no single inter-

---

385 For a discussion on whether the IAHC was representative and its role and authority, see Chapter 5 above. See also WIPO, "An Open Letter from the World Intellectual Property Organisation (WIPO) to the Internet Community Concerning Domain Name Dispute Resolution Procedures under the gTLD-MoU", above n. 341. The open letter states that "WIPO has been criticised as representing large trademark owners only. Nothing could be further from the truth. WIPO's members are national governments, whose trademark offices are concerned with all intellectual property owners...".

386 Johnson and Post, "And How Shall the Net Be Governed?", above n.307.

387 Ibid

388 Ibid
national organisation will ever be able to assemble. In other words, the endorsements of the gTLD-MoU may amount to the “rough consensus” that the Internet community tends to follow. Therefore, an international MoU assembling the relevant international organisations may transform international organisations to feasible instruments for Internet governance.

6.2.2 Should the state remain the key international player?

The mixture of international and private entities supporting the gTLD-MoU thus creates a transgovernmental regulatory body that represents most of the interested parties affected by the changes to the Internet. However, the question as to who has authority, power and accountability is fundamental. The problem with transgovernmental regulatory organisations is that they have no direct power and their functions are primarily consultative. They have no formal basis in treaties. Hence Anne-Marie Slaughter has recently suggested the state should remain as a key international actor allowing and requiring transnational governance to usurp international governance.\(^{389}\) Consequently, the state will provide the necessary power, authority and accountability, and problems can be addressed within the familiar framework of a defined territory. Moreover, she alleges that the domestic institutions can “forge links with their supranational and subnational counterparts, creating the potential for truly

---

\(^{389}\) Slaughter, above n. 269 at 6. She states that “Transgovernmentalism assumes that the primary actors in the international system continue to be state actors”. Harvard professor Lawrence Lessig has recently argued that “the claim that cyberspace is unregulatable is profoundly mistaken”. Lessig’s answer to how the government can impose laws on cyberspace, is that lawmakers must pay close attention to the way software is written. It is software that essentially determines the architecture of cyberspace, he argues. In Lessig’s view, software in cyberspace takes the place of law. So if the courts and legislatures want a hand in fashioning the laws of cyberspace, they must be involved in writing the software, he reasons. Segal, D., “Cyber lawyer wields power in Microsoft antitrust case”, San Francisco Examiner, December 14, 1997, A-3.
global government networks”. The hallmark of transgovernmentalism, she states, is a system in which the principal actors are state units rather than unitary states, interacting horizontally with their foreign counterparts rather than ceding power to their international or supranational equivalents. The result is a new order reflecting the evolution of the nation-state in response to an increasingly borderless world. If the state remains a key player it solves the problem with transgovernmental regulatory organisations having no power. Furthermore, decision-making and implementation would take place at the domestic level as usual.

Slaughter alleges that international governance without the initiative and supervision of the state will not be successful. According to her view, cyberspace will never acquire its own sovereignty. However, this leads to the issue of what kind of governance the gTLD-MoU proposes. The question is how the gTLD-MoU proposal fits in with Slaughter’s view. The gTLD-MoU is an example of international institutions, such as WIPO and ITU, and key transnational Internet actors, such as ISOC and IANA, agreeing to form a governance structure implemented through several regional allocation registries. The gTLD-MoU preserves the original idea of self-governance and provides for a compromise solution. The admin-

390 Slaughter, above n. 269 at 6.
391 Slaughter, above n. 269 at 18.
392 In contrast to Radin’s view, see Radin above n. 346. Slaughter argues that a world government “requires a governmental monopoly on force, a centralised rule-making authority, a clear hierarchy of institutions, and universal membership. That world order is a chimera. Even as an ideal, it is unfeasible at best and dangerous at worst”. Slaughter, above n. 269 at 1.
393 Fitzgerald, above n. 272 at 24.
394 The gTLD-MoU does not require any state involvement, except for the national courts as the last resort in the domain name dispute resolution procedure. See Shaw, R., “Internet Naming Plan Signed: Additional Endorsements Scheduled for Geneva Meeting at the end of April”, above n. 265. Shaw quotes Donald M. Heath, chair of the IAHC, who stated that “using principles of self-governance, the MoU sets up a
istructive structure of the gTLD-MoU does not include any interference of state governments. In other words, it does not adopt Slaughter’s suggestion to obtain power and authority from the state institutions. On the other hand, the gTLD-MoU proposes a centralised decision-making institution. It is a hybrid of commercial entities and international and private organisations. Thus the gTLD-MoU may be categorised as the commercial sector’s attempt to manage the Internet. As a result of the commercial sector having no enforcement power, perhaps Slaughter is right about the need for the state institutions for enforcement and compliance purposes.

The gTLD-MoU proposes a completely new concept of international governance. Ideally, one should build a system that can manage the domain name system on the Internet without building too much bureaucracy, or a bureaucracy too powerful or too regulation-bound. However, the problem with the gTLD-MoU is that it needs a large set of rules and a large bureaucracy to keep the system running. This bureaucracy also needs to have a significant portion of power over a number of areas. As mentioned, the massive domain name resolution system that the gTLD-MoU has built will be difficult to enforce as many governments do not want to give up their own sovereign rights. One possibility is to govern the Internet through two systems. One monolithic and top-down structured system would take care of the structure, that is the maintenance of root servers, handling technical co-ordination among registrars, and doing other technical work. Whereas the other system would handle the substance, that is the non-technical questions involving creation of new gTLDs, representing Internet users, registrars and the organisations that make the Internet run. The latter would instruct the former when new TLDs need to be implemented and other changes affecting the structure are necessary. Moreover, the basic concept should be that the people making decisions should represent the people affected by those decisions. The decision-makers’ power should be limited to the tasks they actually need to perform. More importantly, the state would remain the key actor for enforcement and compliance purposes. In

structure and establishes policies and procedures, for responsible administration of the “generic” portion of Internet domain name space”.

133
other words, international and municipal law would support a new theory - one which is capable of devolving power and decision among various international, public and private entities. State institutions should co-ordinate and co-operate in order to encourage Internet governance by transgovernmental institutions.

In conclusion, international organisations are suited to set Internet policy. The proposed gTLD-MoU, where transgovernmental organisations world-wide are creating an international understanding, is a welcome development. However, the state institutions should provide the necessary authority and power to make transgovernmentalism a workable solution. This paper will argue that international organisation can not realistically govern the Internet without the power of state institutions. Thus the paper proposes that a new theory for Internet governance, where transgovernmental institutions and the state governments co-operate, is the solution. The binding and coercive dimension of law would remain at the national level and both the rule-makers and rule-enforcers would be accountable there.395

395 Slaughter, above n. 269 at 17. Furthermore, she argues that "transgovernmental networks will actually strengthen the state as the primary actor in the international system. The defining attribute of the state has traditionally been the possession of sovereignty - ideally conceived as absolute power in domestic affairs and autonomy in relations with other states". See Slaughter at 28.
THE CONCLUSION AND SOME FINAL REMARKS

A conclusion is just simply the place where someone decided to stop thinking

-- Marsala

The Internet is in transition. Some years ago, business goliaths were found to be asleep at the wheel on the information superhighway.\textsuperscript{396} Today, they are awake and aware of the challenges the Internet poses. Robert Shaw, advisor of the International Telecommunication Union, illustrates this well by declaring:

The Internet is in a painful transition period and appears to be caught in a cross-fire between the tremendous commercial, political, legal and operational interests and anarchistic Net individuals who still want to “do their own thing”. While “chaos” has been legally cited as one of the strengths of the Internet, others are concerned with a certain stability of infrastructure, international comity, respect for legal issues such as trademarks and accountability which is part of the “real world”.\textsuperscript{397}

Up until now, if the domain name you desired were already assigned, your options have been to register for a different name, pay the resale price, sue, or register the name you requested in a different TLD. With this background in mind, the gTLD-MoU proposes a feasible and desirable solution. It includes Internet stakeholders in the governance of the Internet, preserves the idea of self-governance, suggests more TLDs, provides resolution of the conflicts between domain names and trademarks, and implements the solution on a much larger scale than the current RFCs. In other words, the proposal attempts to create a stable environment for commerce on the Internet.

\textsuperscript{396} Brunel, \textit{above n. 165}.

\textsuperscript{397} Shaw, “Internet Domain Names: Whose Domain Is This?”, \textit{above n. 46}.

135
However, the gTLD-MoU may prove difficult to implement. Although it is signed by several international and national entities, there are no sovereign governments that are signatories to it. There may be difficulties with getting all countries to respect, implement, enforce and comply with the gTLD-MoU. Moreover, it is possible that the gTLD-MoU proposal will just be bypassed by the Internet community. In essence, the engineers that run the root servers may ignore a proposal they do not like.398

On the other hand, if the gTLD-MoU is successfully implemented and the seven new TLDs are added to the root servers, the new system is likely to work side by side with the NSI system. No matter what happens to the "com", "net" and "org" TLDs in April 1998, over time, as the new gTLDs acquire reputation and entities start registering in them, the seven new domain names are likely to dilute the popular "com". Then the Internet will have two systems and two different regimes running. Thus the gTLD-MoU provides competition to the NSI monopoly.

As a temporary solution, the best approach would be to leave the domain name disputes to the courts. The Melbourne IT and Uninett "hands-off" approaches are examples of workable policies for domain name allocation and dispute resolution which are currently being utilised. In the long term, however, transgovernmentalism should be encouraged. Transgovernmental regulatory networks produce rules governing subjects that each nation must and does already regulate within its borders. Thus it provides a nationalisation of international law. The binding and coercive dimension of law emerges at the national level, and both the rule-makers and rule-enforcers are accountable at the national level.399 The state will provide legitimacy as the Internet players need a more enhanced legitimacy than the system the Internet currently works on - "rough consensus". Therefore, transgovernmental organisations, states and international and supra-national institutions should co-operate to solve the current vacuum.

398 Frank, above n. 22.
399 Slaughter, above n. 269 at 17.
The present-day emphasis on domain names seems to be at a peak. In coming years search engines, “whois” directories and other metalayers of Internet interaction will develop that make domain names less important and thus not worth fighting over.400 Moreover, the mounting conflicts between trademarks and domain names with global significance are likely to lead to increased pressure for international harmonisation, co-operation and a global trademark system.401 One must remember that in its infancy, the DNS was designed for the exclusive use of academic institutions. Commercial considerations in general, and trademark considerations in particular, were not viewed as relevant.402 The Internet is in an important stage of its life and needs time to adopt to its new role. In the future, the Internet will continue to grow to be an even more vital part of everyday life.

400 Oppedahl, “Remedies In Domain Name Lawsuits: How is a domain name like a cow?”, above n. 66.

401 Shaw, “Internet Domain Names: Whose Domain Is This?” above n. 46.

402 Frank, above n. 22 at 10.
APPENDIX A

THE USAGE OF THE INTERNET

1. The usage patterns of the Internet

According to a survey by Price Waterhouse in June 1997 the top Internet activity is research by searching the WWW.403

<table>
<thead>
<tr>
<th>Activity</th>
<th>Time spent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research</td>
<td>43%</td>
</tr>
<tr>
<td>E-mail</td>
<td>34%</td>
</tr>
<tr>
<td>Game playing</td>
<td>9%</td>
</tr>
<tr>
<td>Online news/mag</td>
<td>5%</td>
</tr>
<tr>
<td>Online banking</td>
<td>2%</td>
</tr>
<tr>
<td>Two-way voice</td>
<td>1%</td>
</tr>
<tr>
<td>Online shopping</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: Price Waterhouse

Conducted: June 1997

As one can see from the table, approximately 43% of the time spent on the Internet was assigned to research. Then comes emailing. Researching and emailing are thus by far the most common activities on the Internet, with 43% and 34% of the time spent, while all the other activities together amount to 18%. According to the Consumer Technology Index in June 1997 by Computer Intelligence, these two most common Internet activities, email and WWW browsing, repre-

2. What Australians do on the Internet

In Australia, according to a recent survey, between 1 million and 1.5 million Australians use the Internet regularly. When examining what Australians do on the Internet, one found that 49% of the use was emailing and 32% of the users utilise the Internet to download software.

<table>
<thead>
<tr>
<th>Use</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>49</td>
</tr>
<tr>
<td>Downloading software/files</td>
<td>32</td>
</tr>
<tr>
<td>Buying goods and services</td>
<td>5</td>
</tr>
<tr>
<td>Reading electronic magazines</td>
<td>15</td>
</tr>
<tr>
<td>Playing games</td>
<td>12</td>
</tr>
<tr>
<td>Interactive discussion</td>
<td>19</td>
</tr>
<tr>
<td>Education services</td>
<td>27</td>
</tr>
<tr>
<td>News and current affairs</td>
<td>19</td>
</tr>
<tr>
<td>General surfing</td>
<td>52</td>
</tr>
</tbody>
</table>

Source: AC Nielsen

404 CyberAtlas, above n. 1.

405 Hannon, K., “Cyberspace nets fewer Aussies than expected”, 20 October, 1997, Courier-Mail (Brisbane, Australia) at 3.

406 Hannon, above n. 3. This was according to a survey by AC Nielsen.
3. Frequency with which WWW users use the WWW

The frequency with which WWW users use the web has also increased dramatically in the last couple of years. According to a survey by FIND/SVP conducted in February to April 1997, in 1995, 36% of the WWW users utilised the WWW daily, whereas 49% of WWW users are daily using the WWW in 1997.407

<table>
<thead>
<tr>
<th>Use frequency</th>
<th>1995</th>
<th>1997</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>36%</td>
<td>49%</td>
</tr>
<tr>
<td>Weekly</td>
<td>45%</td>
<td>39%</td>
</tr>
<tr>
<td>Monthly</td>
<td>13%</td>
<td>7%</td>
</tr>
<tr>
<td>Varies</td>
<td>7%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: FIND/SVP
Conducted: Feb/Apr 1997

These surveys highlight that the utilisation of the Internet is increasing dramatically, both in the number of people accessing the Internet, and the frequency and time they spend on the WWW. The development illustrates the importance of making the Internet user-friendly, making the access to the WWW unruffled, the rates of controversies and litigation low, the rules and policies easy to adhere to, and an internationally accepted system of governance of the Internet.

APPENDIX B

TABLE OF STATUTES

Australia

The Sydney 2000 Games (Indicia and Images) Protection Act 1996 (C’wth)
consol_act/s2000gaipa1996378/s12.html]
(Accessed 8 November 1997)

Trade Marks Act 1995 (C’wth)
[WWW -
cessed 27 August 1997)

Trade Practices Act 1974 (C’wth)
[WWW -
cessed 29 August 1997)

The United Kingdom

The Trade Marks Act 1994

The United States

The US Federal Trademark Dilution Act of 1995 (incorporated in
the Lanham Act paragraph 43 (c) and U.S.C. Title 15 Chapter
22 paragraph 1125 (c))
[WWW - gopher://tad.micro.umn.edu:70/00/bills/104/1/10412951/billtext]
(Accessed 27 August 1997) and
[WWW - http://www.law.cornell.edu/uscode/15/1125.shtml]
(Accessed 27 August 1997)

The US Lanham Act [WWW -
APPENDIX C

TABLE OF TREATIES AND INTERNATIONAL AGREEMENTS

The Madrid Agreement Concerning the International Registration of Marks of April 14, 1891

North American Free Trade Agreement (NAFTA)

The Paris Convention for the Protection of Industrial Property of March 20, 1883, as revised at Brussels on December 14, 1900, at Washington on June 2, 1911, at the Hague on November 6, 1925, at London on June 2, 1934, at Lisbon on October 31, 1958, and at Stockholm on July 14, 1967, and as amended on October 2, 1979


The Agreement on Trade-Related Aspects of Intellectual Property Rights 1994 (TRIPS)
# APPENDIX D

## TABLE OF CASES

### Australia

*Berlei Hestia Industries Ltd v Bali Co Inc* (1973) 129 CLR 353  
*Erven Warnink v J Townsend & Sons (Hull) Ltd* [1979] AC 731  
*Shell Co of Australia Ltd v Rohm & Haas Co* (1949) 78 CLR 601  

### The United Kingdom


### The United States

*Avon v Carnetta Wong Associates*, (unreported, United States District Court for the Eastern District of New York (CV 96 0451)) as discussed in Information Law Alert, “Antidilution Trademark
Law gets first court case”


(Accessed 16 September 1997)


(Accessed 8 November 1997)

(Accessed 5 August 1997)


The Mead Data Central Inc. v Toyota Motors Sales U.S.A. Inc., 875 F.2d 1026, 1035 (2d Cir. 1989)

[WWW – Http://www.jmls.edu/cyber/cases/domain2.html#mtv]
(Accessed 5 August 1997)

Network Solutions, Inc. v Clue Computing, Inc., 1996 WL 697577
(D. Colo.Oct. 29, 1996) as discussed in “Current Developments”
“NSI Cannot Interplead Domain Dispute, District Court Rules”


Playboy Enter v Frena, 839 F.Supp 1552, 1559-61 (MD Fla 1993)

Roadrunner Computer Systems, Inc. v Network Solutions, Inc.,
No. 96-413-A (E.D. Va. complaint filed March 26, 1996, dismissed June 21, 1996)
(Accessed 18 September 1997)

Roadrunner Computer Systems, Inc. v Warner Bros.
(Accessed 16 September 1997)


United States Jaycees v Cedar Rapids Jaycees, 614 F.Supp. 515
(N.D. Iowa 1985) aff’d, 794 F.2d 379 (8th Cir. 1986)

# APPENDIX E

## GLOSSARY

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACP</td>
<td>Administrative Challenge Panels</td>
</tr>
<tr>
<td>CIX</td>
<td>Commercial Internet Exchange</td>
</tr>
<tr>
<td>CORE</td>
<td>Council of Registrars</td>
</tr>
<tr>
<td>CORE-MoU</td>
<td>Council of Registrars Memorandum of Understanding</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FNC</td>
<td>US Federal Network Council</td>
</tr>
<tr>
<td>GATT</td>
<td>General Agreement on Tariffs and Trade</td>
</tr>
<tr>
<td>gTLD</td>
<td>generic Top Level Domain</td>
</tr>
<tr>
<td>gTLD-MoU</td>
<td>generic Top Level Domain Memorandum of Understanding</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IAHC</td>
<td>International Ad Hoc Committee</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>INTA</td>
<td>International Trademark Association</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>iPOC</td>
<td>gTLD-MoU Interim Policy Oversight Committee</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organisation</td>
</tr>
<tr>
<td>ISOC</td>
<td>Internet Society</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>NSF</td>
<td>US National Science Foundation</td>
</tr>
<tr>
<td>NSI</td>
<td>Network Solutions, Inc.</td>
</tr>
<tr>
<td>PAB</td>
<td>gTLD-MoU Policy Advisory Body</td>
</tr>
<tr>
<td>POC</td>
<td>gTLD-MoU Policy Oversight Committee</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comments</td>
</tr>
<tr>
<td>SLD</td>
<td>Second Level Domain</td>
</tr>
<tr>
<td>TLD</td>
<td>Top Level Domain</td>
</tr>
<tr>
<td>TRIPS</td>
<td>Trade-Related Aspects of Intellectual Property Rights</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organisation</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organisation</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>
APPENDIX F

BIBLIOGRAPHY


Baum, A. and Epstein, M., “New Dilution Act Used to Evict ‘Cybersquatters’”

Bazerman, S.H. and Drangel, J.M., “Domain Name Disputes: Trademark Dilution to the Rescue”

Bencivenga, D., “Trademark Dilution”


Buerger, D.J., “Internet naming needs a face-lift to meet real-world needs” (1995) 12 (32) Network World 59


CNET, “Whoever controls the browser controls the Web. But who is that?”


CyberAtlas, “Usage Patterns”
(Accessed 21 August 1997)


Dayal, S., LDL Online, Butterworths, Sydney, 1997

Denninger, K., “DNS Governance Issues”
[WWW - http://www.mcs.net/~karl/http/noi.html]
(Accessed 19 August 1997)

DuWors, R.J., “Truth in Advertising (ACP Style)”
[Email - mailing list “gtld-discuss”] (Received 5 October 1997). [WWW - http://www.gtld-mou.org/gtld-discuss/mail-archive/1263.html]
(Accessed 11 October 1997)

Eliseeva, M., “Is domain name property? Round 2” [Email - “Domain-Policy” mailing list] (Received 22 October 1997)


Evans, J., “Domain names and trademark”
(Accessed 30 July 1997)


Friedman, J.R., “Master your Internet domain name” (1997) 26 (1) *The Magazine for Magazine Management* 64


gTLD-MoU, “Frequently Asked Questions”
[WWW – http://www.gtld-mou.org/docs/faq.html]
(Accessed 20 August 1997)

gTLD-MoU, “Signatories to the gTLD-MoU”
(Accessed 18 November 1997)

gTLD-MoU, “[Second Revised] Substantive Guidelines Concern­
ing Administrative Domain Name Challenge Panels”
[WWW - http://www.gtld-mou.org/docs/sracps.htm] (Ac­
cessed 9 October, 1997)

gTLD-MoU, “Memorandum of Understanding on the generic Top-
Level Domain Name space of the Internet Domain Name
System” [WWW - http://www.gtld-mou.org/gTLD-
MoU.html]
(Accessed 12 October 1997)

World 6

Halpern, S., “International Trade Marks, What Is The Function Of
A Trademark?”
[WWW
http://www.paeman.com/lc/internic/international/itm1.html] (Ac­
cessed 3 September 1997)

Hannon, K., “Cyberspace nets fewer Aussies than expected”
20 October, 1997 Courier-Mail (Brisbane, Australia) 3

Higgs, S., “Registration and Administration of Internet Domain
Names, Comments of Simon Higgs”
cessed 26 August 1997)

Proved?”
[WWW - http://www.ljx.com/trademark/1202s5.html] (Ac­
cessed 1 September 1997)
Hourigan, P., “What’s in a Domain Name?”

Huitema, C. et al, “Not All RFCs are Standards”

IANA, “IANA Overview”

Information Law Alert, “Antidilution Trademark Law gets first court case”

interim Policy Oversight Committee, “Substantive guidelines concerning administrative domain name challenge panels”

International Ad Hoc Committee, “Lottery to Be Dropped from Registrar Selection Process”

International Ad Hoc Committee, “Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs”

International Ad Hoc Committee, “Establishment of a memorandum of understanding on the generic top level domain name space of the internet domain name system”

International Trademark Association, “INTA Internet Subcommittee Proposed Domain Name Registry Policy”
InterNIC, “Domain name dispute policy”
[WWW – http://rs.internic.net/domain-info/internic-domain-6.html]
(Accessed 5 August 1997)

(Accessed 19 October 1997)


Johnson, D.R. and Post, D.G., “And How Shall the Net Be Governed?”
[WWW - http://www.cli.org/emdraft.html]
(Accessed 22 October 1997)

Kenna, C., The TRIPS Agreement: Analysis & Implications. Griffith University, Nathan, Queensland, Australia, 1995

Kennedy, S.D., “Even the IRS has a page on the Internet” (1996) 13 (3) Information Today 50

Kleiman, K.A., “Comments of the Association for the Creation and Propagation of Internet Policies, Inc./Domain Name Rights Coalition and Netaction”

Klein, S.H., “New Attempt At Domain Name Accord”
(Accessed 1 September 1997)
Kouretchian, S., “Internet and Computing, Revised Rules Govern Domain-Name Disputes”  
(Accessed 1 September 1997)

Ladas & Parry Newsletters, “Federal Dilution Trademark Law in the United States”  


[WWW - http://www.isoc.org/intemet-history/]  
(Accessed 15 September 1997)

[WWW - http://www.ljx.com/trademark/p43nation.html]  
(Accessed 1 September 1997)

Loundy, D., “Obscure Experiment of Naming Domains”  

Macavinta, C., “Geneva treaty wins over sceptics”  

Maher, D.W., “Trademarks on the Internet: Who’s in charge?”  
[WWW - http://aldea.com/cix/maher.html]  
(Accessed 21 August 1997)

Melbourne IT, “COM.AU Domain Name Administration General Policy”
(Accessed 3 September 1997)

Messmer, E., “Internet domain names free no more” (1995) 12 (38) Network World 8


Mummery, D.R. et al, “Domain Name Registration: Who should administer?”
(Accessed 1 September 1997)

Nathenson, I.S., “Showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers and other parasites”
(Accessed 22 October 1997)

NetNames, “NetNames Policy Statement on New Generic Top-Level Internet Domains”
(Accessed 16 September 1997)

Network Solutions, Inc., “What They Are Saying About the IAHC Plan”
(Accessed 15 October, 1997)

Network Solutions, Inc., “Internet Domain Name System: Myths and Facts”
(Accessed 16 October 1997)

Network Solutions, Inc., “Secure Internet Administration and Competition in Domain Name Services”
Network Solutions, Inc., “Domain Name Dispute Policy”

Nominet UK, “Comments from Nominet UK on the IAHC Proposals”

Nominet UK, “Rules for the CO.UK domain”

Nominet UK, “Rules for the .UK domain and sub-domains”

Nominet UK, “Nominet UK Dispute Resolution Service”


Oppedahl, C., “You are at risk if your domain name is in COM, NET, ORG, GOV, or EDU”


Oppedahl, C., “Remedies in Domain Name Lawsuits: How is a domain name like a cow?”


Quittner, J., “Billions Registered”


Request for Comment Editor

Rony, E., “Registration and Administration of Domain Names”
(Accessed 15 October 1997)

Rony, E., “gTLD-MoU questions” [Email]
(Received 14 October 1997)


Rutkowski, A.M., “Internet Names and Numbers: Toward a Viable Regime Generic Requirements of a Transition”


Sexton, R., “Registration and Administration of Internet Domain Names, Comments of Richard J. Sexton”
[WWW - http://dns.vrx.net/positions/noi/]
(Accessed 19 August 1997)
Shapiro, S.E., "Use of 'Mead Data' Test Dilutes the Dilution Act"
(Accessed 1 September 1997)

Shaw, R., “gTLD-MoU News November” [Email - “gtld-announce”
mailing list] (Received 14 November 1997)

Shaw, R., “Internet Domain Names: Whose Domain Is This?”
[WWW - http://www.itu.ch/intreg/dns.html]
(Accessed 20 August 1997)

Shaw, R., “Internet Naming Plan Signed: Additional Endorsements
Scheduled for Geneva Meeting at the end of April”

Slaughter, A-M., “The real new world order” (draft dated June 1997,
forthcoming in Foreign Affairs, late 1997)

Smedinghoff, T.J. (ed.), Online Law, The SPA's legal guideline to
doing business on the net, Software Publishers Association/
A-W Developers Press, USA, 1996

Spence, K. (ed.), “Roadrunner, InterNIC’s After You”
(Accessed 16 September 1997)

Squyres, M.M., “New Treaties Add Protection for Well-Known
Marks”
(Accessed 1 September 1997)

Steinberg, D., “Re: Are domain names sold or leased?”
[Email – “Domain-policy” mailing list] (Received 29 October
1997)

Stoodley, J., “Internet Domain Names and Trade Marks” (1997) 19
European Intellectual Property Review 509

Tarjanne, P. “The ITU Responds to New Concepts for Public Policy
in the Global Information Society” (1992) 13 Intermedia

Tebbe M., “Heads up! Internet domain names will be getting goofier” (1997) 19 (8) Info World 62

165
UK Trade Marks Registry, “Registration of Internet Domain Names as Trade Marks” March 12, 1997 (6166) *UK Trade Marks Journal*

Uninett, “Domain name Policy for .no”  
[WWW - http://www.uninett.no/navn/name-policy.html]  
(Accessed 17 September 1997)

US Department of Commerce, “Request for Comments on the Registration and Administration of Internet Domain Names”  

US Department of Commerce, “Notice of Inquiry (NOI) into the Administration and Registration of Domain Names - responses”  
[http://www.ntia.doc.gov/ntiahome/domainname/email]  
(Accessed 20 October 1997)

(Accessed 8 November 1997)

Wells et al, “Internet domain names and TM law”  

*Informationweek* 60

WIPO, “Possible issues to be considered in the context of harmonisation of national and regional laws concerning trademarks and internet domain names”  
[WWW -http://www.wipo.org/eng/internet/domains/tdn/cm/cm ii _2.htm#note1]  
(Accessed 22 July 1997)

WIPO, “Trademarks and Internet Domain Names - Introduction”  
(Accessed 22 July 1997)
WIPO, “Meeting of consultants on trademarks and internet domain names, first session, Feb. 12 to 14, 1997”
(Accessed 22 July 1997)

WIPO, “WIPO meeting of consultants on trademarks and internet domain names”
(Accessed 22 July 1997)

WIPO, “Issues relating to trademarks and internet domain names”

WIPO, “Resolution of Intellectual Property Disputes within the context of the Memorandum of Understanding on the generic Top-Level Domain Name space of the Internet Domain Name System (gTLD-MoU)”
(Accessed 22 July 1997)

WIPO, “Chairman’s summary”

WIPO, “An open letter from the world intellectual property organisation (WIPO) to the internet community concerning domain name dispute resolution procedures under the gTLD-MoU”

WIPO, “Suggestions concerning the proposed WIPO ACP rules and the proposed substantive guidelines concerning administrative challenge panels”
(Accessed 1 August 1997)

WIPO, “The WIPO Arbitration and Mediation Center and Resolution of Disputes Involving Intellectual Property and Internet Domain Names”

**NOTE:** Any RFC can be retrieved with the address ftp://ds.internic.net/rfc/rfcxxxx.txt where xxxx is the RFC number. The gTLD-MoU uses the same approach, see http://www.gtlbmpou.org/docs/rfcs.html.

Emails from three of the mailing lists subscribed to, can be viewed at:

* gtld-announce: Archives: http://www.gtlbmpou.org/gtld-announce/mail-archive/
* gtld-discuss: Archives: http://www.gtlbmpou.org/gtld-discuss/mail-archive/
* Newdom: Archives: http://www.ar.com/lists/newdom
* Domain-Policy does not have an archive.
NSI’s Dispute Policy states in part that:

Network Solutions, Inc. ("Network Solutions") is responsible for the registration of second-level Internet domain names in the top level COM, ORG, GOV, EDU, and NET domains. Network Solutions registers these second-level domain names on a "first come, first served" basis. By registering a domain name, Network Solutions does not determine the legality of the domain name registration, or otherwise evaluate whether that registration or use may infringe upon the rights of a third party.

The applicant ("Registrant") is responsible for the selection of its own domain name ("Domain name"). The Registrant, by completing and submitting its application, represents that the statements in its application are true and that the registration of the selected Domain name, to the best of the Registrant's knowledge, does not interfere with or infringe upon the rights of any third party. The Registrant also represents that the Domain name is not being registered for any unlawful purpose.

Network Solutions does not act as arbiter of disputes between Registrants and third party complainants arising out of the registration or use of a domain name. This Domain name Dispute Policy ("Policy") does not confer any rights, procedural or substantive, upon third party complainants.

4. Revocation. Registrant agrees that Network Solutions shall have the right in its sole discretion to revoke a Domain name from registration upon thirty (30) days prior written notice, or at such time as ordered by a court, should Network Solutions receive a properly authenticated order by a federal or state court in the United States appearing to have jurisdiction, and requiring the Registrant to transfer or suspend registration of the Domain name.

5. Third Party Dispute Initiation. Registrant acknowledges and agrees that Network Solutions cannot act as an arbiter of disputes
arising out of the registration of a Domain name. At the same time, Registrant acknowledges that Network Solutions may be presented with information that a Domain name registered by Registrant violates the legal rights of a third party. Such information includes, but is not limited to, evidence that the second-level Domain name (i.e., not including .COM, .ORG, .NET, .EDU, or .GOV) is identical to a valid and subsisting foreign or United States federal Registration of a trademark or service mark on the Principal Register that is in full force and effect and owned by another person or entity ("Complainant"): 

(a) Proof of such a trademark must be by submission of a certified copy, not more than six (6) months old, of a United States Principal or foreign registration (copies certified in accordance with 37 CFR 2.33(a)(1)(viii) or its successor will meet this standard for registrations in jurisdictions other than the United States ("Certified Registration")). Trademark or service mark registrations from the Supplemental Register of the United States, or from individual states (such as California) of the United States are not sufficient.

(b) In addition to the proof required by Section 5(a), the owner of a trademark or service mark registration must give prior notice to the Domain name Registrant, specifying unequivocally and with particularity that the registration and use of the Registrant's Domain name violates the legal rights of the trademark owner, and provide Network Solutions with a copy of such notice. Network Solutions will not undertake any separate investigation of the statements in such notice.

(c) In those instances (i) where the basis of the claim is other than a Certified Registration described above, or (ii) where the Complainant fails to provide the proof of notice required by Section 5(b), the third party procedures in Section 6 will not be applied.

6. Third Party Procedures. In those instances where a third party claim is based upon and complies with Section 5(a and b), Network Solutions may apply the following procedures, which recognize that trademark ownership does not automatically extend to a Domain name and which reflect no opinion on the part of Network Solutions concerning the ultimate determination of the claim:
(a) Network Solutions shall determine the activation date of the Registrant's Domain name.

(b) If the Registrant's Domain name activation date is before the earlier of (i) the date of first use of the trademark or service mark in the Certified Registration or (ii) the effective date of the valid and subsisting Certified Registration owned by the Complainant, or, if Registrant provides evidence of ownership of a trademark or service mark as provided in Section 5, the Registrant shall be allowed to continue the registration and use of the contested Domain name, as against that Complainant and subject to the remaining terms of this Policy.

(c) If the activation date of the Domain name is after the earlier of (i) the date of first use of a Complainant's trademark or service mark in the Certified Registration, or (ii) the effective date of the valid and subsisting Certified Registration owned by the Complainant, then Network Solutions shall request from the Registrant proof of ownership of Registrant's own registered mark by submission of a certified copy, of the type and nature specified in Section 5(a) above, owned by the Registrant and which was registered prior to the earlier of the date of Network Solutions' request for proof of ownership above or any third party notifying the Registrant of a dispute. The mark provided must be identical to the second-level Domain name registered to the Registrant.

(d) If the Registrant's activation date is after the dates specified in Section 6(b), or the Registrant fails to provide evidence of a trademark or service mark registration to Network Solutions within thirty (30) days of receipt of Network Solutions' request, Network Solutions will assist Registrant with assignment of a new domain name, and will allow Registrant to maintain both names simultaneously for up to ninety (90) days to allow an orderly transition to the new domain name. Network Solutions will provide such assistance to a Registrant if and only if Registrant (1) submits a domain name template requesting the registration of a new domain name; and (2) submits an explicit written request for assistance, including an identification of the Registrant's desired new domain name and the tracking number assigned by Network Solu-
ions in response to the new domain name template, both within thirty (30) days of receipt of Network Solutions' original notice of the complaint. At the end of the ninety (90) day period of simultaneous use, Network Solutions will place the disputed Domain name on "Hold" status, pending resolution of the dispute. As long as a Domain name is on "Hold" status, that Domain name registered to Registrant shall not be available for use by any party.

(e) In the event the Registrant (1) fails to provide the documentation required by Section 6(c) of a trademark or service mark registration within thirty (30) days of receipt of Network Solutions' dispute notification letter, (2) provides Network Solutions written notification that Registrant will neither accept the assignment of a new domain name nor relinquish its use of the Domain name, or (3) fails to take any action or provide any written notice within the times specified in this Section 6, whichever event occurs first, Network Solutions will place the Domain name on "Hold." As long as a Domain name is on "Hold" status, that Domain name registered to Registrant shall not be available for use by any party.

(f) Network Solutions will reinstate the Domain name placed in a "Hold" status (i) upon receiving a properly authenticated temporary or final order by a federal or state court in the United States having competent jurisdiction and stating which party to the dispute is entitled to the Domain name, or (ii) if Network Solutions receives other satisfactory evidence from the parties of the resolution of the dispute.

7. Litigation. In the event that, prior to the Domain name being placed on "Hold":

(a) The Registrant files suit related to the registration and use of the Domain name against the Complainant in any court of competent jurisdiction in the United States, Network Solutions will not place the Domain name on "Hold," subject to the remaining terms of this Policy and pending a temporary or final decision of the court, provided that the Registrant provides a copy of the file-stamped Complaint to Network Solutions. In such cases, Network Solutions will deposit control of the Domain name into the registry of the court. Registrant also shall promptly provide copies of any
and all pleadings filed in the action to Network Solutions upon Network Solutions' request.

(b) The Complainant files suit related to the registration and use of the Domain name against the Registrant in any court of competent jurisdiction in the United States and provides Network Solutions with a copy of the file-stamped Complaint, Network Solutions will not place the Domain name on "Hold," subject to the remaining terms of this Policy, and will deposit control of the Domain name into the registry of the court pending a temporary or final decision of the court.

(c) In both instances, under Section 7 (a and b), Network Solutions will immediately abide by all temporary or final court orders directed at either Registrant or Complainant, without being named as a party to the suit. If named as a party to a lawsuit, Network Solutions shall not be limited to the above actions, but reserves the right to raise any and all defenses deemed.
Earlier Reports in the CompLex series

All reports in the CompLex series may be purchased through the Akademika International Bookshop, Legal Department, Karl Johans gt. 47, 0162 Oslo, Norway, telephone no. +47 22 41 54 50. It is also possible to subscribe to the series through the Norwegian Association for Computers and Law, P.O. Box 6702 St Olavs plass, 0130 Oslo, Norway. Subscriptions may be limited to English language publications, or to «flyers» announcing new reports.

Below, publications for last 5 years are listed. English language reports are printed in **bold face.** A complete list over publications in the CompLex series may be obtained by contacting the Norwegian Research Center for Computers and Law.

CompLex 1/95
Jon Bing
Rettslige konsekvenser av digitalisering:
Rettighetsadministrasjon og redaktøransvar i digitale nett *NOK 368*

CompLex 2/95
Sverre Sandvik
Rettslige spørsmål i forbindelse med utvikling og bruk av standarder innen telekommunikasjon *NOK 178*

CompLex 3/95
Tina Smith
**Legal Expert Systems:**
**Discussion of Theoretical Assumptions** *NOK 278*

CompLex 4/95
Ole Tokvam
Personvern og straffearansvar – Straffelovens § 390 *NOK 198*

CompLex 5/95
Johs. Andenæs
Juridisk utredning om filmen «To mistenkelige personer» *NOK 138*

CompLex 6/95
Jon Bing and Dag Wiese Schartum
**Public Administration and Information Technology** *NOK 348*
CompLex 7/95
Vittorio Frosini
Law and liberty in the Computer Age  NOK 158

ComLex 1/96
Knut-Magnar Aanestad og Tormod S. Johansen
Innsynsrett i elektronisk post i offentlig forvaltning  NOK 218

CompLex 2/96
Stephen Saxby
Public Policy and Legal Regulation of the information Market in the Digital Network Environment  NOK 238

CompLex 3/96
Ellen Lange
Opplysning på spill?
Opplysning, motivasjon, interaktivitet og dataprogrammet Human Quest I  NOK 218

CompLex 4/96
Eva I. E. Jarbekk
Personvern og overføring av personopplysninger til utlandet  NOK 198

CompLex 5/96
Henning Jakhelln
Fjernarbeid
Noen sentrale retningsmål ved nyere former for hjemmearbeid og arbeid utenfor arbeidsgivers øvrige virksomhet  NOK 235

CompLex 6/96
Andreas Mitrakas
A legal Advisory system Concerning Electronic Data Interchange within the European Community  NOK 128

CompLex 7/96
Jon Bing og Ole E. Tokvam
Elektronisk publisering: Utvalgte rettslige aspekter – Rapport på oppdrag av Grafiske bedrifters landsforening  NOK 186

CompLex 8/96
Finn-Øyvind Langfjell
Fjernsynsovervåking og personvern  NOK 138
CompLex 1/97
Therese Steen
Eksemplarfremstilling av litterære
verk til privat bruk

CompLex 2/97
Camilla Sivesind Tokvam
Offentlige anskaffelser av
informasjonsteknologi

CompLex 3/97
Eiliv Berge Madssen
Rettslige spørsmål i tilknytning
til oppgaveregisteret

CompLex 4/97
Halvor Manshaus
Private pengespill på Internett

CompLex 5/97
Christer Krogh
Normative Structures in Natural Artificial Systems

CompLex 6/97
Jon Bing
Rettslige aspekter ved digital kringkasting

CompLex 7/97
Tomas Myrbostad
Elektronisk informasjonsansvar

CompLex 8/97
Ingrid Mauritzen
Avtalelisens etter åndsverkloven § 36
Med særlig vekt på de krav som stilles til organisasjon, jf. § 38 a

CompLex 9/97
Svein Engebretsen
Krav til systemer for forvaltning av immaterielle rettigheter
- Elektronisk handel med åndsverk i et rettsinformatisk perspektiv
CompLex 10/97
Jason A. Hoida
American Telephony: 120 years on the road to full-blown competition
NOK 140

CompLex 11/97
Harald Chr. Bjelke
Rettsslig vern av databaser
NOK 358

CompLex 1/98
Johan Krabbe-Knudsen
Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 A
NOK 198

CompLex 2/98
Guru Wanda Wanvik
Straffbar hacking
Straffelovens § 145 Annet ledd
NOK 238

CompLex 3/98
Katinka Mahieu
INTERCONNECTION
the obligation to interconnect telecommunications networks under EC law
NOK 198
Temaet for denne boken er kjennetegnsretten i «cyberspace» og den internasjonale regulering av internett. Boken gir en analyse av grensen mellom den nasjonale kjennetegnsretten slik vi kjenner den i den virkelige verden og registrering og vern av domenenavn i «cyberspace». Forfatteren gir en oversikt over forsøkene på regulering av domenenavnproblematikken og vurderer hvordan man kan unngå konflikter mellom den nasjonale kjennetegnsretten og kjennetegn på det globale internett. Avslutningsvis analyserer boken mulige løsninger på internasjonalt og nasjonalt nivå.