<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synopsis .......................................................... 9</td>
</tr>
<tr>
<td>The Internet and commerce .................. 9</td>
</tr>
<tr>
<td>Internet domain names ....................... 9</td>
</tr>
<tr>
<td>Trademarks .......................................................... 9</td>
</tr>
<tr>
<td>International domain name registration and dispute resolution .10</td>
</tr>
<tr>
<td>The aims and objectives ....................... 11</td>
</tr>
<tr>
<td>The proposed solution ......................... 11</td>
</tr>
<tr>
<td>Jurisdictions ................................................. 12</td>
</tr>
<tr>
<td>Overview of the chapters ..................... 12</td>
</tr>
</tbody>
</table>

1 Background on the Internet 13
1.1 Definition of the Internet, its history and technical structure ...... 13
1.2 Usage of the Internet.................................................. 15
1.3 The main Internet players .............................................. 15

2 What is a Domain Name?.................................................. 21
2.1 Definitions ........................................................................ 21
2.2 The nature of a domain name –is domain names property? ...... 23
2.3 The allocation of second-level domain names....................... 26
2.4 Background on the problems regarding domain names and trademarks .................................................. 28
2.5 New gTLDs ................................................................... 30
2.6 New .eu country code TLD ............................................ 34
2.7 Overview of the major problems regarding domain names...... 35

3 Background on Trademarks ............................................. 37
3.1 Definition ....................................................................... 37
3.2 Acquisition of trademark rights ....................................... 38
3.2.1 Actual use and registration........................................ 38
3.2.2 What kind of use is required to acquire trademark protection for digital goods? ........................................... 40
3.2.3 Registration of domain names as trademarks ................. 40
3.3 The function of a trademark ........................................... 41
3.4 The rationale of a trademark ......................................... 42
3.5 The different types of trademarks .................................... 42
4 Internet Domain Names and Trademarks

3.6 Trademark infringement and dilution ................................................. 43
  3.6.1 Australia ........................................................................... 43
  3.6.2 The United States .............................................................. 45
  3.6.3 The United Kingdom ....................................................... 47
  3.6.4 Norway ............................................................................. 48

3.7 International harmonisation of the protection of well-known trademarks ..................................................................................... 50
  3.7.1 The Paris Convention .......................................................... 51
  3.7.2 TRIPS ................................................................................ 53

4 The Intersection between Trademarks and Domain Names .......... 57
  4.1 The intersection between trademarks and domain names ............... 57
    4.1.1 The differences and similarities between trademarks and domain names ........................................................................ 57
    4.1.2 The different scenarios of possible conflicts ................................. 59
    4.1.3 Trademark law applied to domain name conflicts .......................... 60
  4.2 Norway – applying law regarding intellectual property infringement to domain name – trademark disputes ..................................... 65
  4.3 Norwegian cases ........................................................................ 67
  4.4 Danish cases ............................................................................. 69
  4.5 The Swedish RENAULT case .................................................... 70
  4.6 The French ALICE case ............................................................ 71
  4.7 Common law countries – passing off ............................................. 71
  4.8 The United States – the NSI policy and the first domain name cases ................................................................................................. 72
    4.8.1 The first come, first served domain name allocation principle ................................................................. 72
    4.8.2 The Intermatic case ............................................................... 72
    4.8.3 The Roadrunner case ............................................................ 74
    4.8.4 The Wire/Wired settlement .................................................... 74
    4.8.5 The Avon case .................................................................... 75
  4.9 The United Kingdom - the Nominet UK policy ....................... 75
  4.10 Australia - the Melbourne IT policy .............................................. 76
  4.11 Two possible defences against allegations of trademark infringement and dilution - groundless threat and the doctrine of trademark misuse ........................................................................ 77
    4.11.1 The United Kingdom ........................................................... 77
    4.11.2 Australia ........................................................................... 79
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.11.3. The United States</td>
<td>79</td>
</tr>
<tr>
<td>4.12 The jurisdiction of courts and the enforceability of judgements</td>
<td>80</td>
</tr>
<tr>
<td>4.13 Remedies in domain name versus trademark lawsuits</td>
<td>81</td>
</tr>
<tr>
<td>4.14 The proposal of a cybermark</td>
<td>82</td>
</tr>
<tr>
<td>5 Icann’s Predecessor</td>
<td>85</td>
</tr>
<tr>
<td>5.1 Background on the gTLD-MoU</td>
<td>85</td>
</tr>
<tr>
<td>5.2 Dispute resolution</td>
<td>87</td>
</tr>
<tr>
<td>6. International Domain Name Registration and dispute settlement – ICANN</td>
<td>89</td>
</tr>
<tr>
<td>6.1 ICANN (The Internet Corporation for Assigned Names and Numbers)</td>
<td>89</td>
</tr>
<tr>
<td>6.1.1 About ICANN</td>
<td>89</td>
</tr>
<tr>
<td>6.1.2 The Shared Registration System</td>
<td>89</td>
</tr>
<tr>
<td>6.1.3 The ICANN accreditation process for registrars</td>
<td>90</td>
</tr>
<tr>
<td>6.1.4 Financial considerations for all registrar applicants</td>
<td>92</td>
</tr>
<tr>
<td>6.1.5 Companies accredited as registrars</td>
<td>92</td>
</tr>
<tr>
<td>6.2 The ICANN Domain Name Dispute Resolution Policy</td>
<td>93</td>
</tr>
<tr>
<td>6.2.1 Introduction</td>
<td>93</td>
</tr>
<tr>
<td>6.2.2 Representations</td>
<td>93</td>
</tr>
<tr>
<td>6.2.3 Requirements for an administrative proceeding</td>
<td>94</td>
</tr>
<tr>
<td>6.2.4 Evidence of registration and use in bad faith</td>
<td>95</td>
</tr>
<tr>
<td>6.2.5 How to demonstrate rights to and legitimate interests in the domain name in responding to a complaint</td>
<td>97</td>
</tr>
<tr>
<td>6.2.6 The Policy and the new gTLDs</td>
<td>97</td>
</tr>
<tr>
<td>6.2.7 Fees</td>
<td>98</td>
</tr>
<tr>
<td>6.2.8 Remedies</td>
<td>98</td>
</tr>
<tr>
<td>6.2.9 Availability of court proceedings</td>
<td>99</td>
</tr>
<tr>
<td>6.2.10 Implementing the decision</td>
<td>99</td>
</tr>
<tr>
<td>6.3 Advantages and disadvantages of the ICANN system</td>
<td>100</td>
</tr>
<tr>
<td>6.4 Domain name cases</td>
<td>101</td>
</tr>
<tr>
<td>7. International Governance of the Internet</td>
<td>111</td>
</tr>
<tr>
<td>7.1 The Internet creates challenges for the current domestic legal systems</td>
<td>112</td>
</tr>
<tr>
<td>7.2 The proposed models for Internet governance: self-regulation or international governance?</td>
<td>114</td>
</tr>
</tbody>
</table>
6 Internet Domain Names and Trademarks

7.2.1 International organisations ...........................................121
7.2.2 Should the state remain the key international player? ..122

8 Domain name Registration in Norway...........................................125
  8.1 Introduction................................................................................125
  8.2 The domain name policy ...........................................................125
  8.3 The new policy...........................................................................126
  8.4 The risk of conflicts ...................................................................127

9. Some Final Remarks .......................................................................129

Appendix 1 .............................................................................................131
  1. Background................................................................................131
  2. Establishment of companies ......................................................131
  3. Trademark registration...............................................................131
  4. Unrestricted domain name allocation ........................................132
  5. Domain name registration in some European countries –
a non exhaustive list...................................................................132
     Norway «.no».................................................................132
     Sweden «.se»...............................................................132
     Denmark «.dk»........................................................................133
     Finland «.fi».................................................................133
     Germany «.de»..................................................................134
     England «.co.uk»............................................................134
     The Netherlands «.nl».........................................................134
     France «.fr» .......................................................................135
     Spain «.es»........................................................................135
     Italy «.it»............................................................................135
     Belgium «.be» .....................................................................136
     Switzerland «.ch».............................................................136
     Austria «.at» .......................................................................136
     Portugal «.pt» ....................................................................137
     Ireland «.ie» ......................................................................137
     Domain name registration: ........................................................137
     Greece «.gr» .......................................................................137
     Luxembourg «.lu».............................................................138
     Croatia «.hr» .....................................................................138
     Yugoslavia «.yu»..............................................................138
     Estonia «.ee».....................................................................138
Hungary «.hu» ................................................................. 139
Slovakia «.sk» .................................................................... 139
Slovenia «.si» ................................................................. 139
Latvia «.lv» ....................................................................... 139
Litauen «.lt» ..................................................................... 139
Poland «.pl» ...................................................................... 140
«.com» ........................................................................... 140
«.org» ............................................................................. 140
«.net» ............................................................................. 140
6. Alternative approaches .................................................... 140

Appendix 2 ........................................................................ 141
SYNOPSIS

The Internet and 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 online. The Internet congregates the world into one single market and with a small investment a business gets access to this world-wide marketplace. With products and services available online, the business can reach virtually everyone. The World Wide Web is easy to access and provides for the convenience of business to business transactions or consumer shopping at home. There is no doubt that the Internet is increasingly important to commerce; this is the new trend and the future of online advertising, selling and purchasing products and services.

Internet domain names
One of the reasons for the growing popularity of the Internet among businesses and consumers is the user-friendly manner of searching the World Wide Web. An international company’s World Wide Web address commonly consists of its trade name with the addition of «.com», or the country code, e.g. «.no». 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 Internet by searching the WWW by domain names. They guess domain names and follow hyper-text 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.

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.

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 often wishes to register a domain name similar to its trademark or company name, which is protected by intellectual property rights (IPRs). However, a regis-
tered trademark is only protected within the jurisdiction (or those jurisdictions) that the registration includes. Thus several businesses around the world may own the same or similar trademarks. Furthermore, the trademark registration system is based on classes of goods and services, so that Dove ice cream and chocolate can co-exist with Dove soap within the same jurisdiction. In contrast, the Internet is global and there is only one domain name under one category of domain names (e.g. »«.com»). Hence there is only one «dove.com».

Another 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 trademark or company name as a part of their Internet address, breach of intellectual property rights, trademark infringement, trademark dilution and unfair competition have been alleged. Thus, trademark law and unfair competition principles were introduced to the unbounded and «lawless» Internet.

**International domain name registration and dispute resolution**

The conflict in the Domain Name System (DNS), where domain name holders and owners of trademarks and other IPRs collide, led to the development of international mechanisms for domain name registration and dispute resolution.

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit international corporation formed in October 1998 to co-ordinate the DNS and domain names under «.com», «.org» and «.net»\(^1\).

The Uniform Domain Name Dispute Resolution Policy (the Policy), adopted by ICANN on 24.10.99, provides an international domain name dispute resolution regime\(^2\). A complaint is filed with an ICANN-approved dispute resolution service provider, such as the World Intellectual Property Organisation (WIPO) Arbitration and Mediation Center (the Center). The Policy is incorporated by reference to the registration agreement with the registrar of the domain name registered under the generic top-level domain names «.com», «.org» and «.net». Thus ICANN dispute resolution is based on a private contractual regime. One is required to submit to and participate in a mandatory administrative proceeding in the event that a third party submits a complaint.

* * *

---

1. Visit www.icann.org (accessed 10.10.00).
2. See www.icann.org/udrp/udrp.htm (accessed 12.10.00).
The aims and objectives
The present book is based on a research project on the Internet Domain Name System (DNS), the tensions between domain names and trademarks and the proposals for Internet governance.

This book will provide an overview of the situations in which domain names and trademarks collide, examine the ICANN domain name dispute resolution system and decisions, and provide a short overview of the domain name registration policy in Norway.

The specific aims of this book are to:

- analyse the legal problems imposed by Internet domain names in general;
- examine the disharmony between domain names and trademarks;
- critically analyse how 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. This will be illustrated by the national allocation policies, such as the Nominet policy in the United Kingdom, the Melbourne Information Technologies Australia (Melbourne IT) policy in Australia and the Norid policy in Norway. The national policies will be contrasted with the domain name registration policies for .com, .net and .org;
- examine the ICANN domain name dispute resolution policy;
- analyse WIPO arbitration decisions under the ICANN domain name dispute policy;
- analyse the domain name’s function as a trademark by using the domain name as intellectual property.

The proposed solution
This book will argue that, in the short term, a temporary system of national policies, such as those utilised by Melbourne IT in Australia and Norid 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 disputes.

In the long term, however, there needs to be an internationally agreed system of governance of the Internet. As the Internet has been in a transition from a lawless playground for «cybernauts» and a network used by academ-

ics, to an international marketplace used by the commercial sector and the citizens in general, there is a need for a system of effective governance on the Internet. The initial system of self-governance did not provide sufficient stability and security in commerce. The Internet needs a policy and legal framework to address the problem of domain names, based on transgovernmentalism, while taking the interests of all Internet stakeholders into account. The international organisations, such as ICANN and WIPO, have provided and will continue to provide for international solutions regarding domain name registration, adding more generic top-level domains and arbitration for domain name disputes. This will ease the tension between domain names and trademarks on the Internet.

**Jurisdictions**

This book will examine the international system of domain name registration and dispute resolution, with the main focus on ICANN and WIPO. Norwegian jurisdiction in particular, and in addition Australian, United Kingdom (UK), United States (US), will be mentioned in some specific instances.

**Overview of the chapters**

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 domain names, provide an overview of the domain name allocation policies, introduce the proposed new gTLDs and examine the background on the conflicts between domain names and trademarks. In Chapter 3 the relevant trademark law will be outlined. 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 provide a short overview of the former international proposals for Internet domain name governance. Chapter 6 will introduce ICANN and the ICANN domain name dispute resolution policy illustrated by WIPO arbitration decisions. Chapter 7 will outline the problems the Internet causes for the current domestic legal systems, analyse whether international organisations would be suited to govern the Internet, and evaluate the proposed models for Internet governance. Finally, Chapter 8 will examine the Norwegian domain name allocation policy in particular and the amendments to the domain name policy.
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 is probably the most powerful means of communication ever invented. It has opened up a «marketplace» of ideas to millions of people around the world for the first time in history.4 Today, the Internet is frequently and widely used for advertising, classifieds, banking, shopping, research, e-mailing, game playing, reading online news and magazines, and other commercial and non-commercial use.

The Internet originated in 1968 in the US experiment called ARPA (Advanced Research Project Agency), and was thus called the ARPANET.5 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 Defence.

---

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. Eventually, as the benefits of the Internet became better known, some private persons formed the Commercial Internet Exchange (CIX). The CIX sponsored high-speed links for commercial traffic on the Internet.

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. 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 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 web server at BA-HR has the numeric address of 195.204.204.14. 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.

---

6. For a good overview of the development of the Internet and how it works, see the US decision American Civil Liberties Union v Reno, 929 F.Supp. 842, 830-845 (E.D.Pa. 1996). Another interesting article regarding the history of the Internet is available at http://www.isoc.org/internet/ (accessed 02.11.00).
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.

1.2 Usage of the Internet
The Internet 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 book a vacation. Furthermore, one may e-mail, chat, and enter discussion groups and newsgroups. In this book, the focus will predominantly be on commercial activity on the World Wide Web.

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 located, and filename is the name of the file that you actually want; 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. In fact, the Internet is not governed, it is co-ordinated. In the beginning, the Internet was run by engineers who voluntarily
took their time to program, manage and maintain the Internet. As a result of the Internet’s origins, the initial bodies which played a role in the operation and self-management of the Internet are of US origin and have a majority, or at least a large number, of US members. As ICANN was formed in 1998, this is beginning to change.

The Internet has been built up, administered and governed by various entities, such as:

1) **The US National Science Foundation (NSF)**

The NSF is an independent US government agency responsible for promoting science and engineering. It provides support and grants for research in networking and communications, including NSFNET. In 1993, NSF created a new organisation to provide specific Internet services, the InterNIC (Internet Network Information Centre). The InterNIC was a co-operative activity between NSF, Network Solutions, Inc. (NSI) and AT&T. AT&T supported directory and database services. NSI sponsored registration services, information and education services, and net scout services. In 1993, the NSF contracted with NSI for the processing of domain name applications under gTLDs. The contract was a five-year agreement, which expired on 31 March 1998. Now the NSI is a registrar for domain names under «.com», «.org» and «.net».

2) **The Internet Society (ISOC)**

The ISOC, a non-profit body established in the US, is, according to its homepage, a «non-governmental, international, professional membership society with more than 150 organisational and 6,000 individual members in over 100 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organisation home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB)».

---

9. See http://whatis.techtarget.com/WhatIs_Home_Page/0,4324,,00.html (accessed 01.11.00) for an explanation of how the Internet works, along with a list of terms and their explanations.
11. See http://www.nsf.gov/home/about/creation.htm (accessed 01.11.00).
12. Visit http://rs.internic.net
13. Visit InterNIC’s information page at http://rs.internic.net.
15. NSF Co-operative Agreement No. NCR-9218742 was the 5 year agreement between NSF and NSI for allocation of domain names under «.com» and several other gTLDs.
3) The Internet Assigned Numbers Authority (IANA)\textsuperscript{18}  
Some Internet standards require administrative implementation in order to allow the Internet to be operational. These include Internet Protocol (IP) addresses. The overall responsibility for this work was initially vested in IANA, which delegated the actual administration of most functions to other bodies. IANA is, according to its homepage, «dedicated to preserving the central co-ordinating functions of the global Internet for the public good».

IANA is a sister body to the Internet Society and was chartered by the Internet Society and the Federal Network Council to assign and co-ordinate the use of numerous Internet protocol parameters. IANA was the central co-ordinator for the assignment of unique parameter values for Internet protocols. Consequently, IANA was the overall authority for the Internet domain names and many other parameters used on the Internet. Today, ICANN assume the responsibilities that previously were vested in IANA.

4) The Internet Engineering Task Force (IETF)\textsuperscript{19} and The Internet Engineering Steering Group (IESG)\textsuperscript{20}  
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 built 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»\textsuperscript{21} 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. The IESG is directly responsible for the actions associated with entry into and movement along the Internet «standards track», including final approval of specifications as Internet Standards\textsuperscript{22}

Previously, the Internet standards were developed through so-called «Request For Comments» (RFCs), which were utilised by the various organisations described in this chapter.\textsuperscript{23} The Requests for Comments were a series of notes, started in 1969, about the ARPANET (the predecessor to the Internet). These governing documents for the Internet discussed many aspects of

\textsuperscript{17} See http://www.isoc.org/isoc/  
\textsuperscript{18} Visit http://www.iana.org/  
\textsuperscript{19} Visit http://www.ietf.org/  
\textsuperscript{20} Visit http://www.ietf.org/iesg.html  
\textsuperscript{21} Visit http://www.ietf.org/overview.html  
\textsuperscript{22} See http://www.ietf.org/glossary.html#IETF  
\textsuperscript{23} 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>.
Internet Domain Names and Trademarks

computing and computer communication focusing in networking protocols, procedures, programs, and concepts, but also including meeting notes, opinion, and sometimes humour.\textsuperscript{24}

5) The Internet Architecture Board (IAB)\textsuperscript{25}
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.\textsuperscript{26}

6) The Internet Corporation for Assigned Names and Numbers (ICANN)\textsuperscript{27}
ICANN is a private, non-profit, corporation formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management and root server system management. IANA and associated entities previously performed these functions under a US government contract\textsuperscript{28}. ICANN is thus the organisation with the superior responsibility for handling Internet domain names.\textsuperscript{29} This international organisation was created by a broad coalition of the Internet’s business, technical, academic and user communities in 1998. ICANN is the single organisation that is authorised to make changes in the root servers. In theory, ICANN may make changes and decisions regarding national domain names (ccTLDs). In practise however, ICANN has been careful not to interfere with the national governance of ccTLDs.\textsuperscript{30}

ICANN accredits registrars for domain names under .com, .org and .net. Moreover, ICANN has implemented a domain name resolution policy for disputes regarding domain names under .com, .org and .net.

7) The Governmental Advisory Committee (GAC)\textsuperscript{31}
In connection with the establishment of ICANN, the organisation associated with an advisory committee of governmental representatives. The advisory

\textsuperscript{24.} 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 1123.
\textsuperscript{25.} Visit http://www.iab.org/iab/
\textsuperscript{26.} For an overview of IAB, see http://www.iab.org/connexions.html
\textsuperscript{27.} Visit www.icann.org.
\textsuperscript{28.} Visit www.icann.org/general/abouticann.htm (accessed 12.10.00).
\textsuperscript{29.} For more details, see RFC 1591 at http://www.ietf.org/rfc/rfc1591.txt (accessed 30.10.00).
\textsuperscript{30.} For more details, see SOU 2000:30.
committee comprises representatives of national governments and public authorities, multinational government organisations and treaty organisations. It has representatives from more than 60 countries.\textsuperscript{32} With an advisory committee consisting of representatives from public authorities from all over the world ICANN has obtained a transgovernmental authority.\textsuperscript{33} Public authorities from all countries in the world are allowed to participate in GAC meetings.

According to the ICANN by-laws, GAC’s role is to «consider and provide advice on the activities of the Corporation as they relate to concerns of governments, particularly matters where there may be an interaction between the Corporation’s policies and various laws, and international agreements».

The GAC shall operate as a forum for the discussion of government interests and concerns, including consumer interests. As an advisory committee it has no legal authority to act for ICANN, however it shall report findings and recommendations to the ICANN Board.

One of the most important activities of GAC has been the proposal of a policy for delegating the governance and handling of ccTLDs to national organisations.\textsuperscript{35}

8) The European Union (EU)
In EU there is currently a working group under the Directorate General Information Society (DG INFSO) regarding Internet related issues. The group works with similar issues as the GAC and the represented countries usually present collective feedback on decisions made in GAC.

In addition, the EU works actively towards the implementation of the new top-level domain name «.eu».

\textsuperscript{33} For a further discussion on the Internet’s need for transgovernmental consensus, see chapter 7.
\textsuperscript{34} Visit the ICANN by-laws at http://www.icann.org/bylaws-09apr99.html (accessed 31.10.00).
\textsuperscript{35} See http://www.noie.gov.au/projects/international/DNS/gac/gacmtg6_communique.htm (accessed 30.10.00) and http://www.icann.org/gac/gac-cctldprinciples-23feb00.htm (accessed 31.10.00).
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 policy; 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 has been in 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
The domain name has a dual nature; it is both a name and an address. Domain names are the plain word 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.microsoft.com». The overlapping system is designed to make the Internet user-friendlier. 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), for example «.com», and a «second-level» domain name (SLD), for example «company.com». In addition, it may have a «third-level» domain name, for example, «company.co.uk». If one reads from right to left, the fields designate the TLD «uk», the SLD «co», and «company» is the third-level domain. There can be an unlimited number of second-level and third-level domain names in each TLD; however, there can be only one of each particular second-level domain name in each top-level domain. Each domain name under the TLD suffix is unique, thus the grant of a registration has effect world-wide. Once «www.BAHR.com» has been registered, it prevents use of that domain name by others anywhere in the world.36

The most widespread use of third-level domain names is within the International Organisation for Standardisation (ISO) 3166 country-code TLD.\(^{37}\) In the country-code TLD, the SLDs often function as categorisers; for example «companyname.com.au», or «universityname.ac.uk». Hence in some country-code TLDs, the third-level domain name is the name that is important to the domain name holder.

Currently, four categories of TLD names exist:

1. **Country code top-level domains (ccTLD)**
   There are more than 240 country code top-level domains\(^{38}\). A ccTLD is a two-letter abbreviation of the name of the country, for example, «.ca» for Canada and «.no» for Norway\(^{39}\). Each country governs its ccTLD, hence the policies may differ from country to country.

2. «.mil», «.edu», «.gov»
   These three TLDs are reserved for US military, educational institutions and governmental agencies only, as historical anomalies from the time when the US was the only country utilising the Internet.

3. «.com», «.org», «.net»
   These three TLDs are referred to as «generic» or «gTLDs». Anyone from any country in the world may register a domain name 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. Their name or acronym must be used as the domain name, e.g. «www.wipo.int».

In addition to the international top-level domain names, there are so-called «domain name havens», such as «.tv», «.as», «.nu» etc. These top-level domains are really country code domain names, however the countries have chosen to open the domain name space to everyone\(^{40}\).

---

37. The International Organisation for Standardisation (ISO) is a world-wide 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 www.iso.ch.

38. According to Yahoo!, there are currently 244 ccTLDs. Visit http://dailynews.yahoo.com/h/ap/20001003/tc/internet_names_1.html (accessed 10.10.00).

39. In Norway, the organisation NORID governs the ccTLD «.no», see www.norid.no.
2.2 The nature of a domain name—is 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 the domain name holder will have against trademark owners.

In the US, the Network Solutions, Inc. (NSI) indicated in its domain name registration policy that a domain name is property. In Network Solutions, Inc. v Clue Computing, Inc., NSI stated 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».

However, if a domain name is property, how can courts transfer domain names 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.

40. The small island Tuvalu is making good profit of its national domain name «.tv». An American company dotTV—pays USD 4 million to Tuvalu each year for the right to sell domain names under «.tv». dotTV has sold more than 100,000 domain names under «.tv». Digital television, broadband services and other telecom business want to register domain names under «.tv». The annual fee for the domain name «sex.tv» is USD 1 million. The company has already sold the domain names «NRK.tv» and «TV2.tv». (Aftenposten 09.10.00).


42. 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 dismiss. 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».
for trademark infringement. What happens in such trademark cases is cancel-
lation of the trademark.

According to Norid, when a domain name is transferred in Norway, the
domain name is formally cancelled and then re-registered in the name of the
new owner. Thus if the outcome of a domain name dispute is that the com-
plainant/plaintiff is entitled to the domain name, or if the domain name is
bought or sold, the transfer is executed in two phases; cancellation and re–
registration.

According to RFC 1591 domain names are «delegated». Thus domain
names registered under the gTLDs, such as .com, are licensed to the owner for
two years at the time. In practice however, entities transfer domain names to
other entities, they sell them, lease them and purchase them as if domain
names were regular property. This illustrates that a domain name may be
said to be property. Moreover, entities go to court to attempt to obtain them.
This practice indicates that once the registrar has granted a domain name, it is
the holders’ to do whatever they want with it.

In Australia the use of a domain name is by licence. Melbourne Informa-
tion Technologies Australia (Melbourne IT)\(^4\), that is the administrator for the
«com.au» domain name space, states in its policy that «The initial licence
period for a com.au domain name is two years».\(^\text{46}\) Furthermore, the Mel-
bourne IT policy states that «The license to use the com.au domain name can-
not be transferred or sold to another party». 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 dis-
puted. The policy states that «The license to use the com.au domain name can
be terminated for reasons outlined in the table below». One of the reasons is
«court decision».\(^\text{47}\) In other words, Australian courts can rule that the domain
name in question should not be licensed to the current licensee, be removed
from the registry, or be licensed to another party. Then the Melbourne IT will
revoke the licence.

---

\(^4\) 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 dele-
gation of the Domain Name», see http://www.nic.uk/drs.html.

\(^44\) As an extreme example of the potential value of a domain name, one may mention the
domain name «business.com», which was sold for USD 7.5 million. An example of a web site
where domain names are bought and sold is www.greatdomains.com (accessed 01.10.00).
The asking price for the domain name «broadband.com» is currently USD 4 million.

\(^45\) For an explanation of Melbourne IT and its role, visit http://www.melbourneit.com.au/


Similarly, in Belgium a domain name cannot be traded. According to the domain name registration policy, the Belgian administrator – DNS BE – grants an exclusive license to the licensee to use the domain name.\footnote{See http://www.dns.be/e/news/index.html (accessed 21.11.00).} «The license is valid for one year and is renewable. The license is personal and not transferable unless the domain name is transferred with the business assets of the licensee. The license for a domain name that is on hold cannot be transferred».

The Belgian administrator may terminate the license if the licensee breaches any of the terms and conditions of the domain name registration, including non-payment of the license fee.

The question whether a domain name is property is a question of whether the domain name has value or whether it can be bought and sold. As ICANN has chosen to have «transfer» as one of its remedies in a domain name dispute, a domain name registered under the international gTLDs, such as .com, is property in the sense that it may be transferred, bought and sold. However, as seen, some countries have chosen to grant licenses and thus prohibit trading in domain names.

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 and Belgium? Or is the entity that has registered the domain name, and who uses it, the legal owner of the domain name? The correct answer must be that the one who has registered the domain name is the owner, unless the administrator merely has granted a license to use the domain name.

In this context, one may raise the question whether a creditor or an administrator of a bankrupt estate may seize a domain name. This is particularly relevant when a so-called «dot com» company go into bankruptcy. Often the company has worked up certain goodwill and consequently the domain name has been built up as a trademark or trade name with a certain value. Not uncommonly, the domain name is the only asset in the «dot com» company.\footnote{Currently, the Norwegian Bankruptcy Act Committee is discussing these issues. Most likely, a domain name may be subject to seizure by a creditor, and in case of bankruptcy the rights to the domain name will be transferred to the bankrupt estate, see the Norwegian Creditors Security Act § 2-2. However, according to Norwegian law, one cannot create a lien on a domain name by contract, see the Norwegian Mortgage Act § 3-4 (2) (b), which is exhaustive and thus cannot be interpreted to include domain names. \cite{KonkursRåd 2001}}

Under Norwegian law, a creditor or an administrator of a bankrupt estate may most likely seize a domain name. In case of bankruptcy, the rights to the domain name will usually be transferred to the bankrupt estate.

See KonkursRåd no 18 - June 2001 “Beslag i domenenavn” by Torjus Torjusen.
2.3 The allocation of second-level domain names

Previously, the gTLDs were administered by the NSI. Today, a significant number of ICANN-approved registrars registers domain names under .com, .net and .org. This section will examine the current domain name allocation policy.

Several commercial entities all over the world have registered a domain name under the «.com» space, and the number of registrations is increasing\(^50\). The main principle in the domain name registration policy is the first come, first served principle. The first entity or person, who apply for a domain name registration, obtains the requested domain name. This principle has been the policy from the very beginning of the allocation of domain names and thus caused most of the problems regarding trademarks.

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. When allocating domain names under gTLDs and most ccTLDs 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.

The first come, first served principle and the fact that a domain name is a limited resource, leads to unique domain name allocations. When the Scandinavian airline SAS decided to go online, an American software company had already registered the domain name «sas.com». Thus SAS registered the domain names «sas.no», «sas.dk» and «sas.se», all of which are routed to the domain name «scandinavian.net».

The same applies to other acronyms, such as «DnB» for «Den norske Bank» and «DNB» for «De norske bokklubber». Both entities would have legitimate interests in the domain name «dnb.no», and the first come, first served principle led to a successful domain name registration by DnB.

In comparison, Melbourne IT\(^51\), 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\(^52\). Secondly, one commercial entity is

\(^{50}\) According to the British company NetNames, the number of registered domain names passed 30 million on 04.10.00, including 18 million domain names registered under «.com». The director of NetNames predicts that it will only take approximately 18 months until 30 million new domain names are registered. Visit http://biz.yahoo.com/rf/001004/104502697.html (accessed 10.10.00).

allowed only one «.com.au» domain name. In contrast, the registrars under gTLDs have no such requirement. 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 cannot be used. The registrars under gTLDs have no such requirement. Finally, the applicant must warrant that «the registration and/or use of the com.au domain name does not breach any third party’s rights (such as those of a trademark holder)». 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.

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, domain names are allocated on a first come, first served basis. The applicant must be an organisation that is registered with the Norwegian Registry of Business Enterprises. Hence individuals may not register second-level domain names, but may register a third-level domain name under the domain name space «priv.no».

Previously, a Norwegian organisation could register only one domain name under .no. However, the Ministry of Transport and Communication has amended the domain name policy expanding the number of domain names per organisation to 15. The policy states that as a general rule, a trademark, product name or other designation cannot be registered as a domain name. However, this will change when the amended domain name policy enters into force. Upon registration, the organisation must sign a statement in which it warrants that the domain name does not infringe upon any third party’s rights.

---

56. The revised domain name policy for .no is available at http://www.norid.no/nypolitikk/25012000/navnepolitikk.html (accessed 02.01.01).
57. EUnet Norge administers the name space «priv.no». The name policy is available at http://193.71.71.193/navn/politikk.html (accessed 12.10.00).
58. The amendment entered into force in February 2001. See the proposal from the Norwegian Post and Telecom Authority http://www.npt.no/norsk/fagomraader/off_telenett/dokumenter/domenenavn.html (accessed 31.10.00). Also see http://www.norid.no/nyheter.html#samferdsel (accessed 22.12.00) for further details.
59. See Chapter 8 below for further details.
The Nominet UK administers domain names in the «.uk» TLD. The first come, first served rule for domain name allocation is maintained in the UK as well. 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 policy for registrations under .com, .net and .org.

2.4 Background on the problems regarding domain names and trademarks

Having defined domain names, considered the DNS and examined some of the current domain name allocation policies, this chapter will narrow the focus to the problems regarding the domain names under the TLD «.com» and trademarks.

The development of the Internet initiated new businesses operating solely on the Internet, whereas old, well-established businesses hesitatingly started to approach the Internet. Some companies started to use the Internet as a traditional printed advertising media, whereas e-businesses used the Internet as a powerful media for building their brands and selling their products. Yet other newly established Internet businesses decided to co-operate or merge with the old, well-established businesses in the real world and thus benefit from their goodwill.

In the last four or five 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. This is due to the fact that companies want to register a domain name that is easy to remember for their customers and potential customers. As mentioned above, it is important to obtain a domain 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

---

60. 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 (accessed 12.10.00).
important. In order to be easy to remember, first of all the domain name need to be short. Many television advertisements end with an Internet address that 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 and company names faced – and will continue to face – problems when they go online, since there is only one domain name under each TLD to grant.63 Examples of weak trademarks, are trademarks that consist of «International», «National», «Australian», «Genesis», «American», «Acme» etc.

The rationale behind the desire to possess a domain 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 Internet by guessing URLs. Hence a potential customer of, for example, IBM would expect to be able to find information about IBM products by typing «www.ibm.com». Furthermore, he or she might try «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 all domain names can remain «guessable». Hence there will need to be an increased reliance on directory services and search engines.

The registration of a trademark, on the other hand, 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 entities 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, Fiesta car and Fiesta 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 Fiesta cars and Fiesta pasta want to go online with the domain name «fiesta.com».

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.

63. 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.
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 increasing⁶⁴. As a consequence, the «.com» TLD name space became crowded. Hence disputes regarding SLD names under «.com» 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.

As the Internet gave rise to several new types of use and misuse of trademarks, consequently, traditional trademark law has been, with more or less success, applied to domain name disputes. Most theorists now agree that the Trademark Act, Company Name Act and Marketing Control Act applies to the clash between domain name holders and trademark owners⁶⁵.

### 2.5 New gTLDs⁶⁶
ICANN has currently been working on the introduction of new gTLDs, such as .biz, .kids, and .sex in addition to the existing .com, .net and .org⁶⁷.

---

⁶⁴. According to the British company NetNames, the number of domain names passed 30 million on 04.10.00, including 18 million domain names registered under «.com». The director of NetNames predicts that it will only take approximately 18 moths until 30 million new domain names are registered. Aftenposten Aften (05.10.00).

⁶⁵. «The Internet and Trade Marks», Knud Wallberg, Sandel Loje & Wallberg, Denmark. For details, see Chapter 4 below.
On 16.07.00, ICANN’s Board of Directors adopted a policy for introduction of new Internet top-level domains (TLDs). The adopted policy called for submission of proposals to sponsor or operate new TLDs by interested persons and organisations. After public comment, these proposals were evaluated and a limited number of proposals were selected for negotiations toward agreements between ICANN and the TLD sponsors and operators.

On 02.10.00, the application period for those seeking to sponsor or operate new TLDs ended. A total of 47 applications were received during the period.

ICANN announced a list of the new suffixes on 16.11.00 and its selections for registry operators for the new top level domains. The applications selected for further negotiation are the following:

- .aero Societe Internationale de Telecommunications Aeronautiques SC, (SITA)
- .biz JVTeam, LLC
- .coop National Cooperative Business Association, (NCBA)
- .info Afilias, LLC
- .museum Museum Domain Management Association, (MDMA)
- .name Global Name Registry, LTD
- .pro RegistryPro, LTD

Global Name Industry is a subsidiary of the Norwegian company NamePlanet. Visit [http://www.digitoday.no/dtno.nsf/pub/dd20001117101740pc97828793](http://www.digitoday.no/dtno.nsf/pub/dd20001117101740pc97828793) (accessed 20.11.00).

---

66. ICANN’s predecessor, the gTLD-MoU, did propose seven new generic top-level domains in 1997. The new gTLDs and the intended fields of use were:
   - «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.


68. Visit [www.icann.org/tlds/new-tld-resolutions-16jul00.htm](http://www.icann.org/tlds/new-tld-resolutions-16jul00.htm) (accessed 12.10.00).

69. For a list of applications, see [www.icann.org/tlds/tld-applications-lodged-02oct00.htm](http://www.icann.org/tlds/tld-applications-lodged-02oct00.htm) (accessed 12.10.00).

70. Visit [http://www.icann.org/announcements/icann-pr16nov00.htm](http://www.icann.org/announcements/icann-pr16nov00.htm) (accessed 17.11.00).
The ICANN is currently negotiating registry agreements with the applicants selected. The agreements will provide the necessary contractual, legal oversight and public policy framework under which the individual registrars must operate.

The board of directors must then approve the negotiated registry agreements. Following that approval, the ICANN board will forward its recommendations to the U.S. Department of Commerce for implementation. The new TLDs are not expected to be operational until at least the second quarter of 2001. The Names Council of the Domain Name Supporting Organization (DNSO) has announced that no one is authorised to pre-register names.

The introduction of «classes» of gTLDs will make the domain names more like trademarks. Many of the suggested suffixes resemble the international trademark classes under the Nice classification, such as .art, .books, .computers, .church, .hotel, .media, .music, .news, .school, .shop, .software, .sports, .biz, .firm, .health, .law, .tel, .travel, .wap. The selected new gTLDs, .aero, .biz, .coop, .info, .museum, .name and .pro, will probably dilute the popular .com gTLD and lead to several new registrations. Especially .biz is expected to become very popular among Internet businesses.

The rationale behind the introduction of the new gTLDs is the massive increase in interest that the Internet is experiencing, especially in the «.com» domain name space. Consequently, it has become crowded at the «.com» TLD space. Latecomers have 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.

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.name», whereas the restaurant McDonald uses «mcdonalds.com» or «mcdonalds.biz». This is similar to the different classes of goods and services in trademark law.

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

71. See http://www.icann.org/tlds/ (accessed 12.01.01).
72. See http://www.icann.org/announcements/icann-pr29sep00.htm (accessed 01.10.00).
73. See Chapter 4 below.
74. See Chapter 3 below.
world-wide chain of hamburger restaurants McDonalds can register the
domain name «mcdonalds.com».

Critics allege that the new gTLDs 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 inter-
national 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 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 nationality 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. How-
ever, 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 domain 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»
would be a better identifier than «propellerheads.se». Moreover, several enti-
ties are world-wide in scope, and do not want to be placed under one particu-
lar country code. The proposal to use the ccTLDs only is feasible in the sense
that it will solve the international administration and governance problems by
making them domestic issues, and could also nationalise the complex trade-
mark conflicts.

However the Internet is global in scope and inevitably one must face the
international issues it raises. Hence the new gTLDs recognises that some
entities merit being in an «international» name space. The question is whether
the seven new gTLDs solve this problem. The number of names available to
specify Internet locations will increase. On the other hand, the new gTLDs
overlap with the existing «.com». For example, a commercial entity may reg-
ister in «.com», «.biz» and «.coop». 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 TLD name space permitting

75. See Chapter 6 below.
more self-selecting categorisation can offer the possibility for trademark owners to register in the gTLDs similar to their trademark class. Thus a better solution than «.biz», might be «.bank», «.flowers», «.food» etc. and instead of «.museum», one could have «.arts», «.movie», «.library» and so on.

Nevertheless, critics fear that trademark owners and businesses 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 will attempt to register their names in all the new gTLDs. Thus the new gTLDs will cause yet another contest between the trademark owners and businesses to register their trademarks and trade names 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.

2.6 New .eu country code TLD

In 1999 the European Commission announced its plans to introduce a new ccTLD: .eu.

This new .eu ccTLD shall serve as an indicator of European identity for European entities present on the Internet, both commercial and institutional. The Commission further noted that the US based .com gTLD was heavily congested and that the national ccTLDs, such as .no, .be, .uk, etc., caused entities to file multiple national registrations. Considering the unification of the European market and the introduction of the Euro, the Commission felt that there was also a need for a common European ccTLD.

In February 2000, the Commission launched a public consultation on how the proposed .eu ccTLD should be set up. Meanwhile, the Commission also has been in contact with the US government and ICANN with respect to the introduction of the .eu ccTLD in the Domain Name System (DNS) and the delegation of the authority to manage the .eu domain.

On 25.09.00, ICANN decided to introduce the .eu domain to the DNS, but it has not yet taken a decision as to who should manage this domain.76 The European Community Panel of Participants (EC-POP) advised that the .eu ccTLD should be managed by a specially created, non-profit organisation.

76. As with the new gTLDs, pre-registration of .eu domain names is not possible. The pre-registration that some companies offer, only amounts to a registration in these companies’ own databases.
2. What is a Domain Name?

The Commission acknowledges that there is a risk that, because of the size of the EU and its economy and the potentially large number of entities requiring .eu domain names, the registry may soon after its opening become just as exhausted as the .com gTLD. For that reason the advice of EC-POP includes the suggestion to create a whole range of second-level domains, such as «.culture.eu» and «.sports.eu» or restricting domains only to trademark owners.77

2.7 Overview of the major problems regarding domain names

To re-focus this book, 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.78

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

The major problems regarding domain names under «.com» and trademarks have been:

- Allocation of domain names;
- Whether trademark law is applicable to Internet domain names and, if, whether a domain name infringes or dilutes an older trademark or company name;
- 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»;

77. The original intention of the Commission was to have the new .eu ccTLD up and running before the end of year 2000, but it is unlikely that this goal will be reached. It is now estimated that the new .eu domain will become operational during spring 2001.

78. 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.
• One business legitimately holds a domain name after registering it, but has no trademark rights in the name. Another business, with trademark rights in that name, desires to use it as its domain name. This is also referred to as «domain name envy». 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 requesting 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 ICANN dispute resolution policy will amend some of the problems regarding domain names registered under «.com», «.org», «.net» and some of the ccTLDs.
3. BACKGROUND ON TRADEMARKS

Aims of chapter 3
The aims of Chapter 3 are to:

- provide an overview of trademark law in Norway and the international era
- 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. When domain names and trademarks collide, the traditional law on intellectual property rights is invoked and applied to the conflict. As mentioned above, Internet domain names, the WWW and its progeny has become a major force in consumer retailing. Hence it is important for businesses to possess a domain name that links to its trademark or trade name.

3.1 Definition
A trademark is a distinctive sign which identifies certain goods or services as those produced or provided by a specific enterprise. Based on a system of trademark registration and protection, consumers can identify and purchase a product or service because its nature and quality – indicated by its unique trademark – meets their needs.

A trademark provides protection to the owner of the mark by ensuring the exclusive right to use it to identify goods or services, or to authorise another to use it in return for payment. The period of protection in Norway is 10 years, but a trademark can be renewed for new 10-year periods indefinitely beyond the time limit on payment of additional fees. Courts may enforce trademark protection by blocking trademark infringement.

Trademarks may be one word or a combination of words, letters, abbreviations and numerals (i.e. word mark, such as «FREIA» or «IBM») and an example of a nickname is «Coke» for Coca-Cola). They may consist of drawings or symbols (i.e. figure marks, such as the stork in the Freia logo or the window icon used by Microsoft). Trademarks may also be three-dimensional signs, such as the shape of the Coca-Cola bottle, or the shape and packaging.

79. See the Norwegian Trademark Act of 03.03.1961 no 4.
of goods. Finally, trademarks may be slogans, such as «Don’t Leave Home Without It», used as distinguishing features.

### 3.2 Acquisition of trademark rights

#### 3.2.1 Actual use and registration

In most jurisdictions, a trademark must either be registered or used in a certain way as a trademark in order to acquire trademark protection.

To obtain a trademark registration, the trademark must be capable of distinguishing the applicant’s goods or services from those of other entities. Thus in order to obtain registration the trademark must be fanciful and have a distinctive stamp, so that consumers can distinguish it as identifying a particular product, as well as from other trademarks identifying other products. It must neither mislead nor deceive customers or violate public order or morality.

An application for registration of a trademark must be filed with the appropriate national or regional trademark office. If a trademark owner desires protection in multiple countries, separate applications must be filed in each country. Filing applications in multiple countries is often complicated, time-consuming and expensive. Thus, in order to simplify the process for applicants who wish to obtain trademark protection in several countries, international treaties have been established. There are a number of international trademark applications filing agreements, such as a Community Trade Mark (EU) application, the Madrid Agreement Concerning the International Registration of Marks (the Madrid Agreement) and the Protocol Relating to the Madrid Agreement concerning the International Registration of Mark (the Madrid Protocol). Quite a few countries are members of such international trademark filing agreements.

The trademark applied for cannot be the same as, or similar to, rights already established by registration or use by another trademark owner. This may be determined through search and examination by the national office, or by the opposition of third parties who claim confusingly similar or identical rights.

---

80. American Express owns the famous trademark «Don’t Leave Home Without It».
81. See the Norwegian Trademark Act § 1 and § 2.
82. For more details, see «Oversikt over norsk varemerkerett», Birger Stuevold Lassen, 2nd edition 1997.
Once a trademark registration is achieved, the trademark will obtain protection within the jurisdiction (or those jurisdictions) which the registration covers.\textsuperscript{86}

In addition to registration, several countries recognise that an entity may acquire trademark rights by use. The trademark must then be used in commerce to distinguish goods or services from those of others. In Norway, in order to establish rights by use, there is a requirement that the entity demonstrates that the mark is well known in the relevant market as its particular trademark for its goods or services.\textsuperscript{87} 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 over the Internet, the use of the trademark extends its market. Consequently, the trademark may acquire trademark rights in new markets. This, however, depends on how the trademark is used and each country’s trademark law. If the trademark is used as a trademark in a new market and may be said to comply with the requirement of usage and acquisition of reputation in that market, new trademark rights may emerge. However, as a result of the global nature of the Internet there are several countries with access to the Internet that does not recognise trademark

\textsuperscript{83} The 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 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.int/treaties/registration/index.html] (Accessed 30.10.00). See also the 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 Madrid Agreement, [WWW - http://www.wipo.int/treaties/registration/index.html] (Accessed 30.10.00).

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 Paris Convention for the Protection of Industrial Property, [WWW - http://www.wipo.org] (Accessed 30.10.00).

\textsuperscript{84} See the Madrid Protocol, June 28, 1989, [WWW - http://www.wipo.int/treaties/registration/protocol-madrid/index] (Accessed 30.10.00). There are currently 67 member states to the Madrid Protocol, including Norway. However, Norway is not a member of the Madrid Agreement.

\textsuperscript{85} Please note that not all countries deny registration of a trademark ex officio. E.g. France does not deny registration ex officio, but Norway does. The practice varies from country to country.

\textsuperscript{86} It is important to note that when one has successfully registered a trademark, one merely has obtained a presumption for a trademark right, which may challenged by a third party afterwards.

\textsuperscript{87} See the Norwegian Trademark Act § 2.
protection by use and acquisition of reputation in a market. Thus it is recommendable to expand the trademark registration to include the markets the trademark is now trading in.88

3.2.2 What kind of use is required to acquire trademark protection for digital goods?

As mentioned above, one can obtain reputation in a trademark through specific use of the trademark in the marketplace. Labelling one’s goods may fulfil the use requirement. However, one must distinguish between tangible goods and digital goods (e.g. software distributed online). With respect to tangible goods, one is required to physically place the trademark, for example a logo, directly on the goods or their packaging. Digital goods however cannot be marked physically. Nevertheless, it should be possible to obtain trademark protection for these kinds of goods as well. For example, one may 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, one may use a trademark by appearing on the web site as a logo. It may then be recommendable to mark the trademark with «TM» – ™ – in order to indicate that this is a trademark, or by «R in a circle» – ® – in order to indicate that this is a registered trademark.

3.2.3 Registration of domain names as trademarks

The question as to whether a domain name can qualify as a trademark, is a question whether the domain name fulfils the requirements of distinctiveness and whether it is used as a trademark. For example, an online magazine may name its web page «cybermagazine.com»; can this domain name acquire trademark protection?

In Norway, one may register a domain name as a trademark providing it fulfils the distinctiveness requirement in the Norwegian Trademark Act. The prefix (i.e. «http://www.») and the suffix (i.e. «.no») of the URL are not considered in the analysis.

In the UK, the UK Trade Marks Registry has issued a statement concerning «Registration of Internet Domain Names as Trade Marks»89. The Registry’s statement explains its current practice concerning applications to register trademarks comprising what appear to be domain names. For example, «netbeer.com» is registered in the UK trademark class 32, and «hyperlink.com» in

88. Notwithstanding the countries one trades in recognise acquisition of trademark rights by use, it is recommendable to register the trademark in order to secure notoriety.
89. See the UK Trade Mark Registry, «Registration of Internet Domain Names as Trade Marks» March 12, 1997 (6166) U.K. Trade Marks Journal.
class 42. 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 similar policy for handling this new breed of mark90. The PTO distinguishes between content, service and link providers. 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.

A problem in connection with trademark registration of domain names and Internet businesses and services, has been how to classify such services. WIPO is currently working on the matter within the framework of the Nice classification (the Nice Agreement concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks of June 15, 1957).91

3.3 The function of a trademark

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 services;

(3) preventing consumer confusion;

(4) assisting consumers in identifying and re-identifying goods and services of a particular producer;

(5) guaranteeing the quality or other characteristics of the goods or services; and

(6) advertising the goods or services.

These functions of a trademark illustrate the importance of protecting trademarks from infringement and dilution.

90. The PTO policy is available at http://www.uspto.gov/web/uspto/info/domain.html.
91. See the Nice Agreement, http://www.wipo.int/treaties/classification/nice/nice.html (accessed 07.02.01). To provide the technical access to Internet customers, i.e. as an Internet Service Provider (ISP), the service is classified in class 38. Other online activities are classified according to the content of the service, i.e. online banking in class 36, online education in class 41, offering of legal services is class 42, offering of «web hotels» is class 42.
3.4 The rationale of a trademark

The rationale behind a system of trademarks is product recognition in the national and international marketplace; the trademark identifies the source of goods. A trademark gives the consumer an indication of the source of origin. 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 may even be a company’s most important and valuable asset. Traditionally the trademark has also ensured quality; the consumer should be sure to get the quality expected. 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.

3.5 The different types of trademarks

One manner of categorising trademarks is to divide them into five different categories: fanciful or coined, arbitrary, suggestive, descriptive and generic terms. Fanciful or coined trademarks are marks without any meaning at the time that they are adapted (i.e. invented words), for example Ajax and Lego (Lego is a composed of the Danish phrase «Leg godt»). Arbitrary trademarks are marks with 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 or a certain effect of the product, such as «Obsession» for perfume and «Vixen» for nail polish. Descriptive marks merely describe a feature of the product. For example, Computerland for a computer store. Generic terms are one type of descriptive marks, such as words that are general or common names for the products to which they are applied. For example, «Beer» for a type of alcoholic beverage or «Orange Juice» for a type of orange juice.

Fanciful marks have a better potential for becoming strong trademarks 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 (i.e. less distinctive) because they refer to the quality or function of the product. Thus they may not be good indicators of origin. On the other hand, a suggestive trademark may become a very strong trademark once it has gained recognition as one. A descriptive trademark is not distinctive and thus it does not qualify as a trademark unless it has gained public recognition.
This recognition is called acquired distinctiveness or secondary meaning. One example of a trademark with secondary meaning is Calvin Klein. Similarly, generic terms cannot be registered as trademarks unless obtained distinctiveness by use. 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.

The chart below depicts the ascending order of distinctiveness and strength of protection of a trademark:

<table>
<thead>
<tr>
<th>Protection</th>
<th>Arbitrary</th>
<th>Descriptive</th>
<th>Generic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fanciful</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.6 Trademark infringement and dilution

#### 3.6.1 Australia

The Australian TM Act section 120 outlines when a registered trademark is infringed. 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 against the infringement allegation that there is no likelihood of confusion or mistake.

Thirdly, section 120 (3) deals with so-called well-known trademarks. A trademark is infringed for the purposes of section 120 (3) if:

- the trade mark is well known in Australia; ⁹⁴ and
- the person uses as a trade mark a sign that is substantially identical with, or deceptively similar⁹⁵ to, the trade mark in relation to;
- goods («unrelated goods») that are not of the same description as that of the goods in respect of which the trade mark is registered («registered goods») or are not closely related to services in respect of which the trade mark is registered («registered services»); or
- services («unrelated services») that are not of the same description as that of the registered services or are not closely related to registered goods; and
- because the trade mark is well known, the sign would be likely to be taken as indicating a connection between the unrelated goods or services and the registered owner of the trade mark; and
- for that reason, the interests of the registered owner are likely to be adversely affected.

This section 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

---

⁹³. Section 120 (3) implements Article 16 (2) and (3) of the TRIPS Agreement.
⁹⁴. For "well known in Australia" see subsection 120 (4): In deciding, for the purposes of paragraph (3)(a), whether a trade mark is "well known in Australia", one must take account of the extent to which the trade mark is known within the relevant sector of the public, whether as a result of the promotion of the trade mark or for any other reason. On the difference between famous and well known marks see WIPO, Final Report on the Internet Domain Name Process (1999) Chapter 4 <http://www.wipo.org>.
⁹⁵. For «deceptively similar» see section 10 of Trade Mark Act.
⁹⁶. For "registered trade mark" see section 6 Trade Mark Act.
infringement by association.\textsuperscript{97} 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{98}

The question is how this can impact on a situation where an owner of a well-known trademark discovers that the registered trademark is used by someone else as a domain name. Furthermore, there is a question as to how the trademark owner can obtain the domain name. Chapter 4 will focus upon these issues.

\subsection*{3.6.2 The United States}
In the US, one can allege trademark infringement on a similar basis to the Australian likelihood of confusion requirement.\textsuperscript{99} 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».\textsuperscript{100} 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’wth), may give similar protection.\textsuperscript{101}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{97} 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 in 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.
\item \textsuperscript{98} 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 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).
\item \textsuperscript{99} See the US \textit{Lanham Act}.
\item \textsuperscript{100} \textit{The US Federal Trademark Dilution Act of 1995}.
\end{enumerate}
\end{footnotesize}
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

(2) likelihood of confusion, mistake, or deception. ¹⁰²

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» ¹⁰³ 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. ¹⁰⁴ On the other hand, based upon a literal interpretation of the Act, there need not be any likelihood of confusion for dilution to occur. ¹⁰⁵ «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. ¹⁰⁶

Under the different state dilution laws, the courts developed the notion of «blurring» or «tarnishment». «Blurring» is typically the whittling away of distinctiveness caused by the unauthorised use of a trademark on dissimilar

---

¹⁰². See the US Lanham Act.
¹⁰³. The Lanham Act paragraph 1125 (c).
¹⁰⁶. 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).
products, while «tarnishment» refers to unauthorised use of a trademark which links it to products that are of poorer quality. 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. One may raise the question whether the use of a famous trademark as an Internet domain name causes dilution of the trademark. This issue will be addressed in Chapter 4.107

3.6.3 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».108 Subsequently, s 10 (6) requires the court to consider whether 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».109

The UK Trade Marks Act section 10 (3) provides that a mark may infringe the rights of a registered trademark holder if used in relation to dissimilar goods or services notwithstanding the absence of confusion, mistake, deception or the likelihood of such. Although not expressly introducing a dilution provision into the Act interpretation of the section does provide for such an application.110 The section reads:


108. 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 public which includes a likelihood of association with the registered trade mark».


110. The connection need not be one that produces consumer confusion: Wagamama Ltd v City Centre Restaurants plc [1995] FSR 713, at 720-721.
[A] person infringes a registered trade mark if he uses in the course of trade a sign which-

is identical with or similar to the trade mark, and

is used in relation to goods or services which are not similar to those for which the trade mark is registered,

where the trade mark has a reputation in the United Kingdom and the use of the sign being without due cause, takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark.

The UK Act does not require use of the mark as a trademark but does require use in the course of trade. It does not use the terms «famous» or «well known», merely the word «reputation». Furthermore, the Act requires unfair advantage of or detriment to the distinctive character or repute of the mark. The section clearly aims to prevent unfair advantage being taken of the value of trademark reputation established through commodification (advertising etc).111

3.6.4 Norway

In Norway, similarly to the UK, there is a likelihood of confusion requirement.112 The question is whether the mark in question is identical to or confusingly similar to another mark.

The likelihood of confusion evaluation is an overall evaluation of the similarity between the marks and the kind of merchandise for which the marks are used. The key issue is whether it is likely that an average consumer would confuse the marks. It is a requirement that a substantial part of the relevant business sector or market may mistake the products for those of another or mistake the products’ commercial origin (direct or indirect confusion). A risk of association is not enough.

When evaluating the likelihood of confusion, some of the relevant factors are:

• the similarity between the kind of merchandise (the nature of merchandise, fellowship in production, fellowship in sales, use or purpose);
• the similarity between the marks (the dominant, visual similarity, phonetic similarity, conceptual similarity);
• the brand awareness in the relevant business sector or market;


112. See the Norwegian Trademarks Act § 4 and § 6 (1).
• the sales method; and
• the elder mark’s distinctiveness.

Consequently, a travel agency called «Solreiser» could have registered the domain name «sol.no», even if the Internet portal Scandinavia Online (SOL) had registered the trademark «SOL».

It is important to note that should someone register a trademark or company name as a domain name with a nonsense supplement only, a court will most likely disregard this. When considering the likelihood of confusion, the dominating parts of the trademark are emphasised (the trademark dominant).

Furthermore, a domain name consisting of elements of a trademark may also be deemed as trademark infringement provided there is a likelihood of confusion. For example would the domain name «manchesterunited-fans.com» infringe upon the trademarks of the famous football club if the Internet pages contained significant commercial material. However, if the Internet page were a fan site only, the conclusion might be different. Furthermore, the domain name «visacard.no» and «visakort.no» would infringe upon Visa the credit card company, whereas a domain name such as «A-visa.no» is most likely not an infringement. When assessing the likelihood of confusion, nonsense additions will be disregarded, however, only to a certain extent. Whereas «coke.no» and «coca.no» would infringe upon the rights of the Coca-Cola company, the domain name «kocolala.no» would not be an infringement. Attempts to exploit others goodwill in a mark would also be a violation of the Marketing Control Act.\textsuperscript{113}

The so-called «Kodak»-doctrine\textsuperscript{114}, provides extended protection for well-known marks. According to this doctrine, a trademark shall be liable to be declared invalid:

• where the trademark is identical with, or similar to, a trademark with better priority, and
• the trademark is to be, or has been, registered for goods or services which are not similar to those for which the earlier trademark is registered, and
• the earlier trademark has a reputation in the kingdom, and
• the use of the later trademark without due cause would take unfair advantage of,
• or be detrimental to, the distinctive character or the repute of the earlier trademark.

\textsuperscript{113} See chapter 4 below.
\textsuperscript{114} See the Norwegian Company Name Act § 3-3 and the Trademarks Act § 6 (2), which implements the EU Trademark Directive 89/104/EEC art. 4, 4, a).
Thus according to the Kodak-doctrine there is no requirement that there is a similarity between the kind of goods or services.

Consequently, a travel agency called «Freia travel» cannot register the domain name «freia.no», as the chocolate manufacturer Freia has a strong trademark and also in all probability enjoys expanded protection according to the Kodak doctrine in Norway. The same applies to the trademark LEGO.\textsuperscript{115} The stronger the trademark the larger difference between the trademark and the domain name is required to avoid likelihood of confusion.

Similar to the US, trademark dilution may also be invoked in Norway. However unlike the US, there is no clear legal basis for a dilution doctrine in Norway. If a domain name is used as a trademark in such a way that the trademark becomes a common description of the product or group of products in question, and thereby weakens the mark, the dilution argument may apply.\textsuperscript{116} The argument must then be based on the Trademark Act § 4 and the Marketing Control Act § 1. If the domain name is not used as a trademark, the Trademark Act is not applicable. The argument must be based on the Marketing Control Act § 1 and general principles of intellectual property law.

### 3.7 International harmonisation of the protection of well-known trademarks

As seen above, trademarks are primarily a national concern.\textsuperscript{117} There is no world-wide international registration of trademarks, however there is an international trend towards harmonisation. Since the Paris Convention in 1883, there has been an extensive international co-operation focusing inter alia on international standard for the recognition of well-known trademarks.

Globalisation and rapid technological change are changing the boundaries of intellectual property rights. The essence of the concept of harmonisation is

\textsuperscript{115} For example, see decision no 00-00240 D by Hadeland og Land Namsrett (court of execution and enforcement) 13.06.00. The defendant had registered the domain name lego.as. The court held that the registration constituted a trademark infringement. The defendant was prohibited from using, transferring or taking other measures regarding the domain name. In addition, the defendant was ordered to take all necessary steps to cancel the domain name. See Chapter 4 below.

\textsuperscript{116} See Chapter 4 below.

\textsuperscript{117} The Paris Convention for the Protection of Industrial Property March 20, 1883. Last amended in 1979. [WWW - http://http://www.wipo.int/treaties/ip/paris/index.html] (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.
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. 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 world-wide scope of the Internet, intellectual property issues have obtained a new dimension.\textsuperscript{118}

As an illustration of the on-going process of international harmonisation of intellectual property rights, this chapter will examine some of the current treaties protecting well-known trademarks.\textsuperscript{119}

3.7.1 The Paris Convention

There are several international treaties to protect well-known trademarks.\textsuperscript{120} However, the different global, regional and bilateral treaties provide different standards of protection. In addition, the phrases «famous trademark» and «well-known trademarks» 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.\textsuperscript{121} In other words, a well-know trademark may to the utmost consequence become famous. 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:

\begin{quote}
(1) \textit{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}
\end{quote}

\begin{itemize}
\item \textsuperscript{118} 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_i_i_2.htm\#note1] (Accessed 22 July 1997).
\item \textsuperscript{119} See Annette Kur, «The WIPO Recommendations for the Protection of Well-Known Marks», IIC Vol. 31, No. 7-8/2000, p 824.
\item \textsuperscript{121} Frederick W. Mostert, Esq., «Well-Known and Famous Marks: Is Harmony Possible in the Global Village», 86 Trademark Reporter 103, 115-116.
\end{itemize}
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.

(2) A period of at least five years from the date of registration shall be allowed for requesting the cancellation of such a mark. The countries of the Union may provide for a period within which the prohibition of use must be requested.

(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.122

The Paris Convention was the first international treaty to pronounce that well-known trademarks are protectable property. 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».

As seen above, Australian law requires that the trademark is «well-known in Australia»,123 Norwegian law requires that the mark is «well known and has a reputation in the kingdom», whereas the US Federal Dilution Act requires that the trademark is «famous».124 Consequently, these different national standards will provide different standards of protection.

122. The Paris Convention for the Protection of Industrial Property, March 20, 1883. The convention is not self-executing, i.e. each country must implement the treaty through its own legislation.  
123. See the Trade Marks Act section 120. 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, NSW, Australia, 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».  
124. The US Dilution Act. In other words, there might be more difficult to obtain the additional protection in the US than for example in Australia.
3. Background on Trademarks

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. «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, \(^{125}\) 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.

3.7.2 TRIPS

Another treaty that provides far greater protection of well-known trademarks is The GATT Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods of the General Agreement on Tariffs and Trade (TRIPS). \(^{126}\) TRIPS is one 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.

---

125. 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.

126. TRIPS was signed by the Members of GATT on 15 April 1994 at Marrakesh, Morocco. View TRIPS at http://www.uspto.gov/web/offices/com/doc/uruguay/finalact.html (Accessed 13 November 1997). Section 2 - Trademarks, Article 15 provides a general definition of the «Protectable Subject Matter» (i.e. trademarks): «Any sign, or any combination of signs, capable of distinguishing the goods or services of one undertaking from those of other undertakings, shall be capable of constituting a trademark. Such signs, in particular words including personal names, letters, numerals, figurative elements and combinations of colours as well as any combination of such signs, shall be eligible for registration as trademarks. Where signs are not inherently capable of distinguishing the relevant goods or services, Members may make registrability depend on distinctiveness acquired through use». 
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 result 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. 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) and in the Norwegian TM Act § 6 (2).
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. How will this impact on the disputes between 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»? And how will the WIPO Arbitration Center handle this when dealing with ICANN domain name disputes?

129. 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 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 European Harmonisation Directive formed the basis of several provisions of the Community Trade Mark Regulation (CTMR), adopted in 1994. 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 DOMAIN NAMES

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, the law applied to intellectual property infringements is utilised.

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 how contemporary trademark law can provide the mechanisms for effective regulation of domain name issues

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 domain names under .com are usually named after the company’s trade name or an acronym thereof. The domain name can tell someone where on the Internet one has been, where one is now, who one is dealing with and how one can find it again. Thus the domain name may create an expectation about the nature of a product or the identity of an entity or organisation. In other words, trademarks and domain names may serve the same function.130

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 con-

fusion. Hence Domino Pizza and Domino Sugar may co-exist in real space. In cyberspace, under the same top-level domain, the second-level 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 «coffee» can be registered as domain names.131

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)132 are likely to collide when they attempt to obtain a domain name under the global domain space .com.

As companies begin to utilise their Internet presence to allow customers to order products including fast food delivery of pizza,133 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 trademarks or service marks in real space. This may change as commerce on the Internet develops further and marks occur that has acquired their reputation solely through the new medium.134

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. Moreover, when trademarks are transported to the new medium, one may argue that a key factor in analysing the likelihood of confusion of a domain name and a trademark will be the «proximity» of the marks. 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.

131. 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.
132. See Chapter 3.5 above.
133. Several companies deliver fast food ordered at their Internet site, see for example Peppes, at http://www.peppes.no (accessed 3 October 2000), who delivers pizza. The same applies to groceries, such as www.rethjem.no (accessed 3 October 2000).
4. The Intersection between Trademarks and Domain Names

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 extension of the service offered in real space. In other words, the marks are more likely to overlap in proximity.

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 domain 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) and a person or entity that has registered the domain name on the first come, first served basis 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. Examples are the Intermatic, Panavision, Kaplan and McDonalds cases. In Norway, examples are the Gjensidige case and the Lego case.

(2) The conflict between two or more owners of weaker trademarks (i.e. low distinctiveness) that both or all desire the same domain name under «.com». Examples are the Prince case and the Roadrunner case.

(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 come, first served principle, with the intention to use it as its legitimate domain name. Later on, the owner of the trademark wants the same domain name when it 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 it desires.

(4) The conflict between two domain name holders with confusingly similar domain names. The emergence of «cybermarks» (i.e. domain names that have obtained reputation entirely through Internet presence) has led to

---

135. This was the case when Dennis Toeppen registered more than 240 domain names. See the Intermatic case, http://eon.law.harvard.edu/h2o/property/domain/IntermaticShort.html.
136. See Chapter 4.8.3 and 4.9 below.
this type of conflict. One example is the conflict between Women’s Wire and Wired Magazine.  

<table>
<thead>
<tr>
<th>Possible Conflicts</th>
<th>Trademark Owner</th>
<th>Domain name holder</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trademark Owner</strong></td>
<td>2) tm and tm</td>
<td>3) dn and tm</td>
</tr>
<tr>
<td><strong>Domain name holder</strong></td>
<td>1) tm and dn</td>
<td>4) dn and dn</td>
</tr>
</tbody>
</table>

### 4.1.3 Trademark law applied to domain name conflicts

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

As the Internet gave rise to several new types of use and misuse of trademarks, consequently, traditional trademark law was applied to domain name disputes. The question is whether contemporary trademark law is applicable and provides the mechanisms for regulation of domain name issues.

Most theorists argue that trademark law, such as the Norwegian Trademark Act, Company Name Act and Marketing Control Act, applies to the clash between domain name holders and trademark owners. A more complex problem, however, is the jurisdiction of courts and the enforceability of judgements.

---

137. The conflict between Women’s Wire and Wired Magazine is examined in Chapter 4.8.4 below.
138. 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 not called «Burger King», but «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 book chooses not to examine the issue.
139. «The Internet and Trade Marks», Knud Wallberg, Sandel Loje & Wallberg, Denmark.
140. See the New Zealand Post case in Chapter 4.12 below.
In several cases, 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. The ICANN domain name dispute resolution policy also links domain names to trademarks and trademark law. The concept of likelihood of confusion, the KODAK-doctrine, the notion of dilution and unfair competition principles is thus applicable to domain name disputes. However, 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 legitimate right to the domain name. Thus these arguments must be balanced in a domain name – trademark dispute.

The US Federal Trademark Dilution Act of 1995, was explicitly enacted, at least in one view, to deal with the conflicts between domain names and trademarks. However, after the new enactment under section 43 (d) of the US Lanham Act, which protects trademarks in general, of the US Anti-Cybersquatting Consumer Protection Act of 1999, there has been less use of – and need for – the Trademark Dilution Act in domain name disputes.

The Anti-Cybersquatting Act gives trademark holders a cause of action against anyone who, with a bad faith intent to profit from the goodwill of another’s trademark, registers, traffics in, or uses a domain name that is identical to, or confusingly similar to a distinctive mark, or dilutive of a famous mark, without regard to the goods or services of the parties.

---

141. The UK Trade Marks Act of 1994. According to section 10 (2), the defendant infringes if there «exists likelihood of confusion on the part of the public which includes a likelihood of association with the registered trade mark».

142. 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.

143. See Chapter 6 below.


145. 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.

146. The full text of the Anti-cybersquatting Consumer Protection Act, enacted 29.11.99, is available at www.mama-tech.com/antipiracy.html (accessed 27.11.00).
It is important to note that the Anti-Cybersquatting Act protects both trademarks and personal names against infringement by domain name pirates.147

As with the ICANN policy, the Anti-Cybersquatting Act outlines indicators of bad faith and legitimate use defences. The Act lists eight factors that can be used in the determination of bad faith registration or intent to profit. The first four would count against a determination of bad faith while the remainder would weigh in favour of a bad faith determination. The factors a court may take into consideration are:

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

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

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

(iv) the person’s legitimate non-commercial or fair use of the mark in a site accessible under the domain name;

(v) the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likeli

147. Under the section «Cyberpiracy protections for individuals», the Act states that:
(A) CIVIL LIABILITY- Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.
(B) EXCEPTION- A person who in good faith registers a domain name consisting of the name of another living person, or a name substantially and confusingly similar thereto, shall not be liable under this paragraph if such name is used in, affiliated with, or related to a work of authorship protected under title 17, United States Code, including a work made for hire as defined in section 101 of title 17, United States Code, and if the person registering the domain name is the copyright owner or licensee of the work, the person intends to sell the domain name in conjunction with the lawful exploitation of the work, and such registration is not prohibited by a contract between the registrant and the named person. The exception under this subparagraph shall apply only to a civil action brought under paragraph (1) and shall in no manner limit the protections afforded under the Trademark Act of 1946 (15 U.S.C. 1051 et seq.) or other provision of Federal or State law.
hood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(vi) the person’s offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for substantial consideration without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services;

(vii) the person’s intentional provision of material and misleading false contact information when applying for the registration of the domain name; and

(viii) the person’s registration or acquisition of multiple domain names which are identical to, confusingly similar to, or dilutive of trademarks or service marks of others that are distinctive at the time of registration of such domain names, without regard to the goods or services of such persons.

It is possible to obtain an award of statutory damages limited to USD 100,000 per domain name. In one case, a domain name pirate had registered five domain names that infringed upon a trademark. The trademark owner was awarded statutory damages amounting to USD 500,000.

Furthermore, the Anti-Cybersquatting Act provides «in rem jurisdiction». Consequently, if the domain name is registered under an alias name, and the requirements in the Act is fulfilled, it is possible to sue the domain name itself. As a remedy one may be awarded the rights to the domain name even if the domain name registrant is nowhere to be found.

The first case decided under the new Act, the Sporty’s case, the court found bad faith in a situation where «a competitor X of Company Y has registered

148. The Anti-Cybersquatting Act states that:
«The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if-- (i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c); and (ii) the court finds that the owner-- (I) is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or (II) through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by-- (aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and (bb) publishing notice of the action as the court may direct promptly after filing the action.»

149. For a good presentation of the new act, see http://eon.law.harvard.edu/h2o/property/domain/legislation.html (accessed 27.11.00).
Y’s trademark as a domain name and then transferred that name to Subsidiary Z, which operates a business wholly unrelated to Y». Sportsman’s Market - a catalogue company targeted at aviation enthusiasts uses the logo and trademark «sporty’s» to identify its catalogues. Omega Engineering, a catalogue company that sells mainly scientific instruments, registered the domain name «sports.com». Omega’s owner is a pilot who was familiar with Sportsman’s catalogues and the Sporty’s trademark. Nine months after registering «sportys.com», Omega transferred the name to a subsidiary it created to grow and sell Christmas trees. It named the subsidiary Sporty’s Farm and sold the rights to sportys.com to the subsidiary.

The case was originally filed under the Trademark Dilution Act, but the Anti-Cybersquatting Act was passed before the appellate court rendered its decision. The appellate court determined that new law applied on appeal. It then found that there was more than enough evidence in the record to demonstrate bad faith. Neither Sporty’s Farm nor Omega had any intellectual property rights in sportys.com and Sporty’s Farm did not begin use of the name in a bona fide offering of goods or services until after the litigation began. Most importantly, however, the court held that although the «unique circumstances» of the case did not fit neatly within the bad faith factors enumerated by Congress, there was sufficient evidence to find bad faith. For instance, the court found that Omega planned to enter into direct competition with Sportsman’s in the pilot and aviation consumer market and thus their primary intent was to prevent Sportsman’s from using the sportys.com domain name. The court found that Omega created the Sporty’s Farm business solely to find a use of the sportys.com name in some commercial fashion and thus keep the name away from Sportsman’s and protect against a possible infringement claim. Because the domain name was registered prior to the passage of the Anti-Cybersquatting Act, the court refused to award damages to Sportsman’s Market.

In general, trademark infringement or dilution may be established if use of the domain name can be said to constitute use of the trademark, i.e. to distinguish goods or services used in the course of trade from other products. An example that illustrates that trademarks are believed to 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 Internet.

Nevertheless, one may argue that merely registering a domain name may not be sufficient conduct to constitute infringement or dilution. It has been discussed as to whether offers to sell the domain name to its legitimate holder constitute «use» of the trademark. Moreover, even posting a web page under the domain name may not be actionable. One may argue that there is no particular reason to suppose that a person happening to surf to the domain name «mcdonalds.com» would associate the site with a source of hamburgers. If one cannot buy hamburgers at the site, one may argue that there is no confusion between the domain name and the trademark. More importantly, the world is full of individuals named McDonald, any of whom might have registered such domain names. In other words, the notion of dilution and likelihood of confusion in traditional trademark law does not always satisfactorily cover the situation in cyberspace.

For example, in the US Intermatic case, 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 the domain name holder – Toeppen – and Intermatic provided. Further, there was no evidence of consumer confusion. From this reasoning one can clearly see that the court argued the domain name – trademark dispute similar to a traditional trademark infringement case.

4.2 Norway – applying law regarding intellectual property infringement to domain name – trademark disputes

As mentioned above, in all probability a domain name must be used as a trademark or trade name in order to be deemed as an infringement and cause a likelihood of confusion as described in the Norwegian Trademark Act and the Company Name Act. A mere blocking of the domain name cannot amount to trademark infringement. Especially in the US, but also in Norway, persons have «stocked up» on domain names identical or similar to famous trademarks and company names, but never actually used the domain names. In those cases, national courts – and now also the ICANN/WIPO domain name dispute arbitration – have «constructed» use. For example, courts

---

152. See ICANN decision regarding «Madonna.com» in Chapter 6 below.
154. For example, see the «Bridget Jones» case, discussed in Chapter 6 below. The decision is published at http://arbiter.wipo.int/domains/decisions/html/d2000-1000.html (accessed 09.10.00).
have stated that if the domain name holder intend to sell the domain name to the rightful owner or offer the name for sale to the public, this constitutes use of the domain name.\footnote{\text{155. It seems that Norwegian courts too construct intention to sell equals use of the domain name. See the Lego case below.}}

On the other hand, the Norwegian Marketing Control Act § 1 and § 8a may be applicable to a blocking of someone else’s trademark. However, the Act only applies to entrepreneurs.\footnote{\text{156. The ICANN domain name dispute policy omits non-commercial use of the domain name from the policy. See Chapter 6 below.}} Should a private person block a trademark as a domain name, or use it in a non-commercial manner only, the Act would not apply.\footnote{\text{157. Should a private person block a trademark as a domain name and offer the domain name for sale at an excessive price, this may amount to blackmail or extortion and punishable in accordance with the Norwegian Criminal Act § 266. If a private person registers a domain name identical or similar to a trademark and do not blackmail the rightful owner or use it as his own non-commercial homepage, it is difficult to prevent him from doing this. If it is important to the rightful owner to own the domain name, the trademark owner may pursue negotiations with the domain name holder to tempt him to sell the domain name.}}

If the domain name is used as a trademark, in a case of conflict between domain names and trademarks, the regular law applicable to intellectual property breach will apply, such as the Marketing Control Act, the Company Name Act and the Trademark Act. The Norwegian Trademarks Act § 4 and § 6 (1) applies to a domain name – trademark conflict provided that the domain name is used as a trademark.

In other words, one must consider two factors when registering a domain name;

(i) Could the domain name be deemed as confusingly similar to a trademark or company name registered or used by a third party?

(ii) Could the registration of the domain name be deemed as detrimental to good business practice between entrepreneurs?

As discussed in chapter 3 above, the question of likelihood of confusion is a question as to whether it is likely that an average consumer would confuse the marks.

As regards the assessment of «good business practise» in the Norwegian Marketing Control Act § 1, one may register a domain name similar to a trademark as long as it is not registered and used with the intent to dilute or weaken the trademark, or exploit the goodwill in the mark.
4.3 Norwegian cases

In a case before Stavanger Namsrett (court of execution and enforcement) – the Bailine case – the court held that a franchisee’s registration of the franchisor’s trademark and trade name was detrimental to good business practice between entrepreneurs, the Marketing Control Act § 1.\(^{158}\) The franchisee had registered the domain names «bailine.no», «bailine.as» and «bailine.co.uk». The franchisor, Bailine Scandinavia AS, was the owner of the trademark (logo) BAILINE. It is interesting to note that even if the franchisor had only registered the trademark as a figure mark (logo), the court held that the word mark BAILINE had acquired trademark rights by use, the Trademark Act § 2. The franchisee had offered the domain names for sale, and prior to the judge pronouncing a decision the franchisee actually transferred the domain name «bailine.no» to another company. The court noted that registration of a domain name for the purpose of selling the domain name might constitute exploitation of the goodwill in the mark. As the domain names were registered with the knowledge of the franchisor’s trademark rights, motivated by a possible payment for a transfer of the domain names to the franchisor or other entities, and without consulting the franchisor, this was inconsistent with the Marketing Control Act § 1. The franchisee was prohibited from using, transferring or taking other measures over the domain names and other domain names containing the word «bailine», and the franchisee was ordered to take all necessary steps to cancel the domain name registrations.

In the Lego case, the defendant had registered the domain name «lego.as».\(^{159}\) The court held that the registration and use of the domain name constituted a trademark infringement. The defendant had offered the domain name for sale to the plaintiff. He also claimed that he intended to make an Internet portal for kids. LEGO is a famous trademark registered in most countries throughout the world. Lego also argued that the trademark LEGO had acquired such reputation and goodwill that it enjoyed the extended protection in the Kodak-doctrine, the Trademark Act § 6 (2). The court held that the registration of the domain name was a trademark infringement inconsistent with the Trademark Act § 4. The reasoning was that as a consequence of the exclusive rights of a trademark owner, the registration and use of the domain name «lego.as» is an infringement of the trademark LEGO. The defendant was prohibited from using, transferring or taking other measures.

\(^{158}\) See Stavanger Namsrett (court of execution and enforcement) case no 00-00530 D 14.11.00.

\(^{159}\) See Hadeland og Land Namsrett (court of execution and enforcement) case no 00-00240 D 13.06.00
regarding the domain name and was ordered to take all necessary steps to cancel the domain name registration.

However, it was not clear from the judgement whether the domain name was actually used or merely registered. The defendant stated that he intended to use the domain name as an address for an Internet portal for kids. One may raise the question whether the Trademark Act § 4 is infringed when the domain name is merely registered. The domain name is blocked, but not used as a trademark or likely to cause consumer confusion. Furthermore, strictly speaking, the Marketing Control Act § 1 is not applicable when a private person has registered the domain name. Since the defendant had offered the domain name for sale to the plaintiff, one may argue that the Norwegian Criminal Act § 266 should have been used in this case.

In the Gjensidige case, Gjensidige Forsikring sued a person that had established a company called Gjensidige Software, and who had registered the domain name «gjensidige.com».\(^{160}\) Gjensidige argued that there was a likelihood of confusion (the Trademark Act § 4 and the Company Name Act § 3-2) and that the defendant’s use of the name constituted a breach of Gjensidige’s intellectual property rights. Gjensidige also argued that the name «Gjensidige» had acquired such reputation and goodwill that it enjoyed the extended protection in the Kodak-doctrine (the Trademark Act § 6 (2) and the Company Name Act § 3-3).

The court found that there was a likelihood of confusion. Furthermore, the court found that the registration and use of the domain name «gjensidige.com» was detrimental to good business practise. However, in this case it was indisputable that the defendant had registered «gjensidige.com» with the only purpose to harass and damage Gjensidige Forsikring.

The court held that Gjensidige Software was prohibited from using, transferring or taking other measures regarding the domain name «gjensidige.com» or other domain names containing «Gjensidige». In addition, Gjensidige Software was deemed unauthorised to use «Gjensidige» as a part of its company name and/or trademark for its goods and services. Gjensidige Software was ordered to pay litigation costs amounting to NOK 6,000.\(^{161}\)

Another recent case regarding domain names is the “IT Fornebu” case.\(^{162}\)

---

160. See Oslo Namsrett (court of execution and enforcement), case no 98-431 D 18.02.98.
161. It is interesting to note that to date (21.11.00), according to a whois search, the domain name gjensidige.com still is registered in the name of the defendant – Gjensidige Software. However, there is no match for «Gjensidige Software» in the Norwegian Register of Business Enterprises.
162. Tønsberg Namsrett case no 01-705 D dated 14.06.01.
4.4 Danish cases

In Denmark, several judgements have concluded that a domain name may infringe upon a trademark. In one decision from Copenhagen City Court, 02.12.97, the court held that neither the Danish Trademark Act nor the Company Name Act was applicable. However use of the domain name was considered a violation of the Marketing Control Act § 1 and general principles of law. It is worth mentioning that this case was a clear «piracy case», in which the defendant had registered the plaintiff’s company name as a domain name and tried to sell the domain name to plaintiff at an excessive price.

In another Danish case, the 118 case, a company called ITCOM AS had registered the domain names «118.dk» and «1118.dk». In Denmark, the telephone directory services number provided by Tele Danmark is «118» (similar to the Norwegian 180). ITCOM AS had purchased Tele Danmark’s database and launched a free information service on the Internet.

Tele Danmark had registered 118 as a part of a trademark logo. The court found that Tele Danmark also had acquired trademark rights to 118 as a word mark by use. The registration and use of the domain name «118.dk» by ITCOM AS was thus deemed inconsistent with the Trademark Act § 4 and the Marketing Control Act § 1. The two companies provided identical services. The difference that ITCOM provided the service via Internet was of no consequence; it was nevertheless a likelihood of consumer confusion. Furthermore, the difference that ITCOM provided the service for free was of no consequence.

The domain name «1118.dk» was deemed likely to cause confusion and inconsistent with the Trademark Act § 4 as it was merely an insignificant difference from Tele Danmark’s protected trademark «118».

In another case, the Beologic case, a private person had registered the domain name «beologic.com». Baan Nordic AS (previously Beologic AS) had registered the trademark BEOLOGIC and used «Beologic» as its secondary business name. The court found that the domain name was registered with the intent to sell it to Baan Nordic AS for an excessive price. Such action, stated the court, must be deemed as a business detrimental to good marketing practise, the Marketing Control Act § 1.

163. A good Internet site for viewing Danish intellectual property cases is www.ipb.dk.
164. See decision from Copenhagen City Court, 02.12.97, no 1583/97.
165. See decision from Copenhagen City Court, 22.01.98, no FS25688/97.
166. See decision from Østre Landsret (County Court), 26.11.99, no B-3553-97.
167. It is interesting to note that the court characterised the «action» (registering domain name with the intent to sell it to the rightful owner) as a «business», even though it was carried out by a private person. It seems that the court constructed a «business» in order to use the Marketing Control Act which is only applicable between entrepreneurs.
The court noted that as long as the domain name was not offered for sale to others than the trademark owner or owner of the secondary business name, or otherwise used for marketing of goods or services, no breach of the Trademark Act § 4 could be established.

In the Yellow Page case, a company had in 1997 registered the company name WWW.YELLOWPAGE.DK ApS and the domain name «yellow-page.dk». The company offered sale and marketing of advertisement space on the Internet. The plaintiff, Yellow Page Reklamebureau, had since 1984 operated an advertising agency. The advertising agency had registered a trademark logo with the text «Yellow Page graphic design and communication» in classes 35 and 42.

The court found that the dominant of the plaintiff’s trademark logo was the words «Yellow Page». Thus there was a risk that the defendant’s domain name and company name would be confused with the plaintiff’s company name and trademark. The court found that the two companies offered identical services and business operations. The fact that the defendant offered its services via a database and that the information service was offered via the Internet did not eliminate the likelihood of confusion with the plaintiff’s company name and trademark.

In the Rolex case, a person who purchased and sold used Rolex watches registered the domain name «rolex.dk». Montrex Rolex AS sued the person, and alleged that the use of the domain name was unauthorised and that the person could not register any domain name containing the phrase «rolex». The court upheld both contentions. The court held that the use of the domain name constituted unauthorised use of the Rolex trademark. However, it is not clear from this case whether a domain name such as «saleofused-rolex.dk» would be deemed as unauthorised use of the Rolex trademark.

4.5 The Swedish RENAULT case

In Sweden, a company named Renault Consulting AB was denied registration of the domain name «renault.se». The company complained to the committee for review of domain name registrations (NÖD). NÖD ruled that the domain name «renault.se» could be registered by Renault Consulting AB due to the fact that there was a strong connection between the company and the French mother company Renault SA.

168. See decision from Copenhagen City Court, 31.10.97, no FS 18066-97.
169. See Sø- og Handelsretten, 18.08.00. A summary of the case is available at Lov & Data no 63/September 2000.
170. Nämden för överprövning av domännamn (NÖD).
4. The Intersection between Trademarks and Domain Names

4.6 The French ALICE case
In France, there was a domain name dispute between two companies with identical company names. The first company, ALICE SNC (established 1957), had in 1975 registered ALICE as a trademark for marketing services. The other company, ALICE SA (established 1966), offered software programs. The latter had registered the domain name «alice.fr». The French domain name registration policy is based on the «first come, first served» principle.

The former company sued due to likelihood of confusion. The court held that the domain name should be cancelled. The appeal court reversed the decision. The appeal court used the specialisation principle, which allows two identical trademarks to co-exist if they do not cause a likelihood of confusion. The appeal court held that there was no likelihood of confusion between a software company and an advertising agency172.

4.7 Common law countries – passing off
In common law countries, protection of well-known trademarks developed from the «passing off» action. «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, 173 are said to be required of a successful action. «Passing off» prohibits someone from exploiting other people’s goodwill. It is clear that by registering other entities’ trademark or trade name, or a similar trademark or trade name, one deliberately creates confusion in the marketplace and amongst users as to the origin of the site. In so doing, one is passing off the site as that of the other entity’s by seeking to imply that there is a conception, development and maintenance of the other entity’s site. This attempt to take advantage of other entities’ goodwill is considered passing off and will not be accepted by a common law court.

171. See Lov & Data no 57/March 1999 for an overview of this and other NÖD-cases.
172. See Lov & Data no 59/September 1999 for an overview of the case.
4.8 The United States — the NSI policy and the first domain name cases

4.8.1 The first come, first served domain name allocation principle
As a result of the first come, first served principle — first used by the NSI — 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 wake up and realise that they need to go online. Consequently, when they woke up, they found that the most logical domain name («theircompanynname.com») was taken. This resulted in a number of lawsuits in the middle of the 1990s, many of which were legitimate; for example, the Candyland, Kaplan and Intermatic 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. 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.

4.8.2 The Intermatic case
As an illustration of domain name grabbing, the case Intermatic, Inc. v Dennis Toeppen highlights the issue of domain name hijacking of famous trademarks. Intermatic Incorporated v. Dennis Toeppen. See chapter 4.8.2 below. 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. This was the first cross-border domain name case and was litigated in the UK. See Chapter 4.11.1 below. 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. MTV Networks v Curry, 867 F.Supp. 202 (S.D.N.Y. 1994).
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». The owner of the trademark «Intermatic» thus sued Toeppen, alleging trademark infringement, trademark dilution and related causes of action.

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. The US Federal Trademark Dilution Act 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.

178. The Intermatic Incorporated v. Dennis Toeppen. 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».

179. The Intermatic, Inc. v Dennis Toeppen. The court actually calls Mr. Toeppen a «cybersquatter». 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) The Computer Lawyer 20 at 20.


182. Critics argue that the transfer of the domain name relief did not follow from the Federal Dilution Act. See Chapter 2.2 above.
4.8.3 The Roadrunner case
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.

In the Roadrunner case, 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.

4.8.4 The Wire/Wired settlement
Another scenario occurs when two domain names are confusingly similar. This happened in the out-of-court settlement between Wire and Wired. Wire, a computer network devoted to women’s issues, registered the domain name «wire.net». Wired, a cyberspace magazine, registered 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».

It is worth noting that they changed not only their domain name, but also their business name in real space. This helps minimising any likelihood of confusion. The dispute is interesting, as it is an early predecessor to the kind

---

183. 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.

184. 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.


186. See http://www.law.georgetown.edu/lc/internic/recent/rec5.html#wired.

187. In return, Wired agreed to pay half the cost of the name change expenses, such as redoing online graphics and identity materials.
of cybermark conflicts that will arise in the future.\footnote{An owner of a cybermark has acquired reputation based entirely on Internet activities. See Chapter 4.14 below.} 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.

### 4.8.5 The Avon case

Avon Products filed one of the first suits under the US Federal Trademark Dilution Act of 1995.\footnote{Avon v Carnetta Wong Associates (unreported, United States District for the Eastern District of New York (CV 96 0451)). See Chapter 3 above about the stated intention of the Act and what «dilution» is.} 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. 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.\footnote{In Norway, 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.}

As mentioned in Chapter 3 above, when using the US Trademark 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.\footnote{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. See also Chapter 3 above.} 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.

### 4.9 The United Kingdom - the Nominet UK policy

*The domain name «co.uk» is one of the most common domain names after the «.com». Hence it is important to have an overview of the Nominet UK’s*
rules. Also, the first legal ruling on the domain names in the UK, the case Pitman Training Limited v Nominet UK ¹⁹², will be examined.

Today, the Nominet UK has a hands-off approach to domain name disputes.¹⁹³ Previously, Nominet had a hands-on approach and offered a domain name dispute service to third parties that alleged that a name registered under .uk infringed upon their intellectual property rights. One may ask whether it was desirable that the domain name disputes were resolved by the same entity as the one that granted them. Eventually, Nominet surrendered and handed the disputes over 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 web 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.

4.10 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 revokes a domain name «where a court of competent authority determines that the domain name should not be allocated to the applicant...».¹⁹⁴ In other words, it leaves the disputes to the courts.

In the Sydney 2000 case, the Asia Pacific Internet Company (APIC) had registered the domain name «sydney2000.net». The Australian Sydney Organising Committee for the Olympic Games (SOCOG) proposed to take action under the Sydney 2000 Games Protection Act, the Trade Practices Act for «misleading and deceiving» and common law for «passing off». The action raised a number of issues. The Sydney 2000 Games Protection Act was enacted after APIC registered the domain name. Thus the question was, can a government legislate to override domain names allocated by the US registrar 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 represent a commercial value beyond the Olympics.

The Melbourne IT has the most efficient and effective domain name allocation policy. Conflicts between domain names and trademarks have been solved 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.

4.11 Two possible defences against allegations of trademark infringement and dilution - groundless threat and the doctrine of trademark misuse

This section will focus on the defences against allegations of breach of intellectual property rights.

4.11.1. The United Kingdom

In the UK, Prince plc v Prince Sports Group, Inc. is an illustrative case. The case is based upon the UK Trade Marks Act of 1994 s 21 on groundless threat and the doctrine of trademark misuse.
threats of infringement. Section 21 is the counterpart of the Australian TM Act section 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 argued 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 current NSI policy procedure, to avoid litigation.199

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 trademark 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...

199. The Prince case. 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».

Previously, the NSI had a domain name dispute resolution procedure, under which it was possible to place the domain name on hold and then transfer the domain name if the domain name holder could not produce evidence that showed an adequate legitimate interest in the domain name.
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.\textsuperscript{200}

The Prince case illustrates that section 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 itself to blame if the proceedings result in relief being granted against it.

\textbf{4.11.2. Australia}

In Australia, the TM Act section 129 is the counterpart of section 21 in the UK Act. The relevant subsections in section 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{201}

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

\textbf{4.11.3. The United States}

In the US, there is no provision in the Lanham Act similar to the UK s 21 and the Australian section 129.\textsuperscript{202} However, the question can be raised whether the doctrine of trademark misuse may be used as a defence similar to the groundless threat defence.

\textsuperscript{200} The Prince case. 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...».

\textsuperscript{201} The Trade Marks Act 1995.

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. Courts may extend the broad equitable doctrine of trademark misuse to prevent trademark owners from complaining unjustifiably 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.

According to the trademark misuse case United States Jaycees v Cedar Rapids Jaycees, 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». The courts have yet to find 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. 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».

4.12 The jurisdiction of courts and the enforceability of judgements

In New Zealand, the NZ Post case is a good example of jurisdiction and enforceability in domain name disputes. A New Zealand citizen had registered the domain name «nzpost.com», and the web page contained some material that overlapped with goods or services offered by NZ Post. New Zealand Post (NZ Post) is a large postal services company in New Zealand and sued for passing off and breach of the Fair Trading Act. The court held

204. Quoted in Davidson and Engisch.
205. Davidson and Engisch. 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.
206. See EIPR 1999, issue 8, pages 417-419. The judgement in the NZ Post case was pronounced 18.12.98.
that the continued existence of the «nzpost.com» would lead to confusion and there was at least a prima facie case for breach of the Fair Trading Act. Furthermore, the court held that it had jurisdiction to issue an injunction against the defendant and that its order was enforceable against him despite the fact that the domain name was attached to a host computer outside New Zealand. Thus the defendant was restrained from directly or indirectly being involved with an Internet service or site incorporating or using the words NZ Post as a domain name or part thereof or any similar domain name.

4.13 Remedies in domain name versus trademark lawsuits

Having looked at the intersection between domain names and trademarks, and finding that trademark law is 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?

Theorists have criticised several US cases where the courts have transferred the domain name to the trademark owner.207 The 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.208 When analysing three cases where the courts ordered a transfer of the domain name, one finds that in the three cases, Actmedia, Intermatic and Panavision, the trademarks are truly

207. There is no remedy in trademark law or dilution law that calls for transfer of a domain name. See Chapter 2.2 above regarding the nature of a domain name.

208. Oppedahl, http://www.patents.com. «Remedies in Internet domain name trademark lawsuits». 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, 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. 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.
unique.\textsuperscript{209} 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{210} Another relevant factor is whether the domain name holder is doing anything with the domain name.\textsuperscript{211}

With this in mind, theorists have suggested that a transfer of domain name relief is appropriate only if the trademark being asserted is unique or coined. 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.

4.14 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{212} Disputes between cybermarks, such as the Women’s Wire and Wired Magazine case, will continue to occur increasingly as commerce on the Internet becomes more common.

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. 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.

\textsuperscript{209} 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{210} In the Intermatic and Panavision cases, Mr Toeppen had registered more than 240 domain names.

\textsuperscript{211} In the Toeppen cases, much attention was paid to this question. The Federal Trademark Dilution Act, requires that there is «commercial activity», hence the Act should not be applicable to a passive domain name holder. See Chapter 4.8.2 above.

\textsuperscript{212} Flint, D., «Internet Domain Names, Proposal for a cybermark.» (1997) 13 (3) Computer Law & Security Report 163 at 163. A cybermark is defined as a domain name whose reputation attached to it depends entirely on Internet presence.
unless the owner can establish a 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.

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. When the Internet provides a stable and predictable environment for business and commerce, cybermark law may evolve.213 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. 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. Future will show whether ICANN has the authority to implement such new intellectual property law regime on the Internet.

213. Disputes between deceptively similar domain names have previously been determined under local law. This places a complainant in a difficult position of having to enforce its rights in multiple jurisdictions. The ICANN domain name dispute policy and WIPO arbitration center might change this. See Chapter 7 below for different models for dealing with Internet governance at the international level.
5. ICANN’S PREDECESSOR – THE FIRST INTERNATIONAL PROPOSAL FOR DOMAIN NAME ALLOCATION AND DISPUTE SETTLEMENT – THE GTLD-MOU

This chapter will outline the first proposed solution to the problems in the DNS and the inconsistencies between domain names and trademarks - the gTLD-MoU. This proposal was rejected. However, it was ICANN’s predecessor and the first proposed solution to domain name problems at the international level. Thus the gTLD-MoU is an important part of the Internet history.

5.1 Background on the gTLD-MoU

In 1993, NSI entered into a five-year agreement with the US government which granted NSI a monopoly on the domain name registration in the gTLDs .com, .net and .org. Historically, several attempts were made to stop NSI’s monopoly of the domain name registration in the most popular gTLD, .com. One attractive development, was the Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System (the gTLD-MoU).

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 was issued on February 4, 1997 and the gTLD-MoU 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. The Internet Society then decided to undertake the domain name problems using this draft.


216. The Postel Draft was 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.
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. The initial signatories of the document were the IANA and the ISOC. The ITU acted as a depository for the gTLD-MoU and published the list of signatories.

Several entities signed the gTLD-MoU, however the gTLD-MoU did never enter into force. Interestingly, several US entities signed the MoU, in spite of the general opposition against the gTLD-MoU in the US.

The gTLD-MoU purported to provide an instrument for signatories to advise on future policy evolution of the global DNS. In a legal context, however, the question was what would give the gTLD-MoU force: contract law, private international law or public international law? MoUs are not treaties; they do not engage the executive or the legislature in negotiations, deliberation, or signature. They merely affirm existing links among regulatory agencies based on their common functions and commitment to the solution of problems.

According to the gTLD-MoU preamble, the document should provide an «international policy framework» through the establishment of a «self-regulatory structure under a voluntary MoU». However, the gTLD-MoU was a policy intended to be binding on the activities of the registrars and the SLD name holders within the gTLD. In other words, it tried to constitute both a private international law contract of association and a form of public international administrative regulatory regime. The gTLD-MoU was an interesting hybrid because of the mix of sovereigns and non-sovereigns signing it. It purported to bring public and private actors together in a corporatist style of international governance structure.

218. The gTLD-MoU section 4 provided 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.
220. There was a large opposition against the gTLD-MoU.
222. The «Council of Registrars for generic Internet domain names Registrars» (CORE). CORE was the entity comprising registrars for domain names under the suggested new gTLDs. Visit http://www.core.gtld-mou.org.
5. Icann’s Predecessor – THE FIRST International Proposal for Domain Name allocation and dispute settle-

If the gTLD-MoU was a contract, however, the question was which country's laws would govern the contract. Regarding the «Council of Registrars for generic Internet domain names Registrars» (CORE), the CORE-MoU art. 8 (d) stated: «This CORE-MoU shall be governed by the laws of Switzerland». Art. 8 (e) referred disputes arising out of the CORE-MoU to UNCITRAL arbitration under Swiss law. However, there was no such provision in the gTLD-MoU.

Another issue that arose, was on the basis of which laws would the dispute resolution be adjudicated. Further, how would the signatories to the gTLD-MoU be bound by changes? What would keep them bound to changes in the future? As stability was crucial, these questions were lively discussed before the gTLD-MoU could enter into force.

Nonetheless, the gTLD-MoU process was scheduled to begin operation on 15 February 1998, prior to the expiry of the NSI contract. The new CORE system was scheduled to be fully operational by 30 September 1998. Due to the harsh critics, the US Department of Commerce issued a counter-proposal in 1998. This proposal was criticised by the EU. Hence the five-year agreement with the NSI, which originally was due to expire on 31.03.98, was prolonged until 2000. Simultaneously, the process towards the establishment of the ICANN commenced.

5.2 Dispute resolution
As discussed in detail above, the first come, first served principle led to disputes between domain name holders and third parties. The NSI had a «hands-on» approach to address these domain name disputes. However, this approach did not work satisfactorily. The gTLD-MoU had a different approach to the problem.

The CORE-MoU stated that the registrars should not attempt to solve any disputes between domain name holders and third parties. Instead, the «Administrative Domain Name Challenge Panels» (ACPs) should perform this duty.

226. See http://www.democracy.net/archive/09251997/
227. See the gTLD-MoU section 8 - Administrative Domain Name Challenge Panels.
Further, the gTLD-MoU stated that «Registrars shall be obligated to honour all decisions of ACPs». Consequently, there should 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 moved registrars entirely out of the line of fire. This was an important alteration and the ICANN system is clearly based on this idea.
6. INTERNATIONAL DOMAIN NAME REGISTRATION AND DISPUTE SETTLEMENT — ICANN

6.1 ICANN (The Internet Corporation for Assigned Names and Numbers) and the Shared Registrations System (SRS) for domain names

6.1.1 About ICANN

The ICANN is, according to its web page «a non-profit international corporation formed in October 1998 to oversee a select set of Internet technical management functions previously managed by the US Government or by its contractors and volunteers». Specifically, ICANN is assuming responsibility for co-ordinating the management of the domain name system (DNS) the allocation of IP-address space, the assignment of protocol parameters and the management of the root server system.

6.1.2 The Shared Registration System

The so-called Shared Registration System (SRS) is a system for domain name registration in which competitive registrars register domain names under «.com», «.net» and «.org». The SRS was created in spring 1999 through the initiative of the United States Department of Commerce. Under this domain name registration system, competing ICANN-accredited registrars register domain names utilising one shared central registry. The SRS registry is operated and maintained by Network Solutions Inc. (NSI).

There is no limit on the number of registrars that may register names using the SRS. However, there is a requirement that every business desiring to

---

228. Visit www.icann.org (accessed 12.10.00).
229. According to ICANN’s homepage, see www.icann.org/registrar/accreditation-overview.htm (accessed 04.10.00).
231. NSI has no longer monopoly on the registration in .com, .net and .org. However, NSI has been granted a monopoly by the US government to be the register and have the administrative role of .com, .net and .org. NSI is also one of the major registrars for domain names in .com, .net and .org.
232. For an updated list of accredited registrars, visit www.icann.org/registrar/accredited-list.html (accessed 13.10.00).
become a registrar in the «.com», «.net» and «.org» top level domains must first become accredited for the purpose by ICANN.

6.1.3 The ICANN accreditation process for registrars
The ICANN accreditation process for registrars for the «.com», «.net» and «.org» top-level domains includes several steps\(^{233}\):

(i) Apply for registrar accreditation
   The business must complete an ICANN registrar accreditation application and send it to ICANN along with a non-refundable USD 1,000 application fee.
   The application review process usually takes between four and six weeks. Applications with very specific, thorough answers and all necessary supporting documents may be processed more quickly.

(ii) Receive notification that the business qualifies for registrar accreditation
   ICANN will inform the business by e-mail of its decision to accredit the business or not. ICANN will announce the accreditation along with contact information for the company on its web site.

(iii) Sign the accreditation agreement with ICANN
   The last step in the ICANN registrar accreditation process is for the business to execute a registrar accreditation agreement with ICANN. The current version of the agreement was approved November 4, 1999 by the ICANN Board of Directors. This is a standard document that all registrars sign with ICANN.
   After the business has signed the agreement, ICANN then notifies NSI. NSI will then contact the business within 3 to 5 days in order for the business to start signing agreements with it and obtain the SRS software.

(iv) Receive fully executed agreement for ICANN and pay accreditation fee
   The invoice for the annual fixed portion of the accreditation fee is USD 5,000.

(v) Sign confidentiality agreement with NSI
   NSI requires the business to sign a confidentiality agreement before the business is given access to certain SRS software and documentation. The agreement is contained in the NSI Registrar License and

\(^{233}\) Visit www.icann.org/registrars/accreditation-process.htm (accessed 07.02.00).
Agreement which NSI send the business after it has been notified of the accreditation by ICANN.

(vi) Obtain assurance of performance
The version of the NSI Registrar License and Agreement currently approved for the use by NSI requires registrars to have in place an USD 100,000 performance assurance, such as a bond or insurance.

(vii) Arrange to obtain an appropriate SSL license
The business systems communications with the SRS will employ a secure socket layer interface (SSL). This may require the business to obtain a software license from a third party vendor.

(viii) Prepare to sign a registrar license and agreement with NSI
NSI will send the business the Registrar License and Agreement. This must be signed and returned to NSI.

(ix) Prepare to pay NSI's license fee
NSI’s SRS software license fee is an USD 10,000 one-time fee. The business must pay the fee before it can connect with the SRS-system.

(x) Obtain the SRS software and documentation from NSI

(xi) Prepare the business systems to interface with the registry

(xii) Test the business software
NSI has established a test platform for use in testing the business’ systems interoperability with the SRS.

(xiii) Verify the business systems’ functionality

(xiv) Make arrangement with NSI for pre-payment of registration fees
NSI require that before the business may actually register domain names through the SRS, the business must make arrangements to pay the registry fees through a Letter of Credit, deposit account, or other terms acceptable to NSI.

(xv) Complete preparation of the business’ agreement with customers and uniform domain name dispute policy
The ICANN registrar accreditation agreement provides some guidance on these requirements. ICANN has adopted a uniform dispute resolution policy (the Policy) that all accredited registrars are required to follow.
(xvi) Inaugurate the service

After the above steps have been completed, the business should be in a position to begin offering services to the public.

6.1.4 Financial considerations for all registrar applicants

As seen above, the registrars must undertake significant financial considerations and pay fees to both ICANN and NSI to become accredited\textsuperscript{234}.

Fees to ICANN:

- USD 1,000, non-refundable application fee to be submitted with the application
- USD 5,000 annual accreditation fee
- USD 70,000 in working capital requirement
- Quarterly accreditation fee paid once the business begins registering domain names

Fees to NSI:

- USD 10,000, one time SRS software license fee to be paid before the business can connect to the SRS system
- USD 100,000 performance bond or performance assurance insurance

Payment arrangements with NSI must be completed before the business can begin registering domain names. In addition, NSI will require that the business provide security for the registry fees that incur, such as by deposit account in a Letter of Credit.

6.1.5 Companies accredited as registrars

There are currently 159 companies that are accredited as registrars by ICANN\textsuperscript{235}. As accredited registrars these companies will compete in the market for domain name registration services by participating in the shared registry system (SRS), which allows multiple ICANN accredited registrars to register domain names ending in «.com», «.net» and «.org».

\textsuperscript{234} Visit www.icann.org/registrars/accreditation-financials.htm (accessed 07.02.00).
\textsuperscript{235} For an updated list, visit www.icann.org/registrars/accredited-list.html (accessed 20.11.00).

One example of an accredited, operational registrar is the Norwegian company Active ISP.
6.2 The ICANN Domain Name Dispute Resolution Policy

6.2.1 Introduction
The Uniform Domain Name Dispute Resolution Policy (the «Policy»), adopted by ICANN on 24.10.99, outlines a process for international domain name dispute resolution. ICANN requires their accredited registrars for «.com», «.net» and «.org» to make the Policy part of the registration agreement. The registration agreement is a contract between the registrant (i.e. the domain name holder) and the registrar. The registrant is then contractually bound to submit to the Policy if a complaint is filed. Thus this process represents a private contractual system of dispute resolution.

ICANN has accredited dispute resolution service providers. One such ICANN-approved dispute resolution service provider is WIPO. A complaint under the Policy may only be filed with an ICANN-approved dispute resolution service provider.

The Policy sets forth the terms and conditions in connection with a dispute between the domain name holder and any third party over the registration and use of an Internet domain name.

As mentioned, all registrars in the «.com», «.net», and «.org» top-level domains are contractually bound to follow the Policy. In addition, some administrators of country code domain names have decided to submit domain name disputes under the Policy; such as «.as», «.nu» and «.tv».

6.2.2 Representations
When registering a domain name under «.com», «.net», and «.org», one represents and warrants that:

1. the statements that you made in your registration agreement are complete and accurate;

---
236. The Uniform Policy can be found at www.icann.org/udrp/udrp-policy-24oct99.htm (accessed 12.10.00).
237. In the US, there is also the US Anti-Cybersquatting Consumer Protection Act, which lists eight factors that can be used in the determination of bad faith registration or intent to profit. See chapter 4 above.
238. Currently, there are four approved dispute resolution service providers. For the purposes of this book, WIPO will be used as an example of approved dispute resolution service provider. A list of ICANN-approved dispute resolution service providers can be found at www.icann.org/udrp/approved-providers.htm (accessed 05.10.00).
239. For a complete overview, visit http://arbiter.wipo.int/domains/cctld/index.html (accessed 05.10.00).
2. to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party;

3. you are not registering the domain name for an unlawful purpose; and

4. you will not knowingly use the domain name in violation of any applicable laws or regulations.

It is thus the domain name holder’s responsibility to determine whether the domain name registration infringes or violates someone else’s rights. This representation constitutes the background and basis for a possible complaint from a third party.

### 6.2.3 Requirements for an administrative proceeding

Section 4(a) of the Policy sets out the three elements which must be present for a proceeding to be brought against the respondent, and which the complainant must prove to obtain a remedy. It provides as follows:

«a. Applicable Disputes. You [the Respondent] are required to submit to a mandatory administrative proceeding in the event that a third party (a «Complainant») asserts to the applicable Provider, in compliance with the Rules of Procedure, that

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

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

your domain name has been registered and is being used in bad faith.»

It is important to note that in the administrative proceeding, the complainant must prove that each of these three elements is present.

The phrase «identical» means the domain name must be same as a trademark once the TLD is removed, for example domain name «toshiba.net» and trademark «Toshiba».

The phrase «confusingly similar» means so similar as to be confusing, taking into account the relevant factors, for example domain name «worldcup2002.com» and trademark «world cup», or domain name «reuters.com» and trademark «reuters». In other words, one compares the

---

240. This is similar to the statement on must submit under the NORID domain name registration policy in Norway.
241. Note that these factors are similar to those in the Norwegian Trademark Act § 4, the Company Name Act § 3-2 and the Marketing Control Act § 1 and § 8a.
dominant of the domain name with the dominant of the trademark and assesses whether they are so similar as to be deemed confusing.

The phrases «trademark or service mark» means registered trademark, registered prior to the domain name registration. It also may comprise the situation where the trademark is registered subsequent to the domain name registration, and even unregistered trademarks, in which case the trademark protection is acquired by use. Furthermore, this term may comprise the situation when there is an unregistered trademark that is a personal name.

In an arbitration procedure under the ICANN Policy regarding the registration of a domain name under «.com», «.org» and «.net», the Administrative Panel («the Panel») shall decide the case on the basis of the Policy, in compliance with the Rules of Procedure, and any rules and principles of law that it deems applicable.

### 6.2.4 Evidence of registration and use in bad faith

Section 4(b) of the Policy identifies circumstances in which the Panel may deem the registration and use of a domain name to be in bad faith. These include circumstances that amount to cyber-squatting, restraint of trade by an owner, disrupting competitors’ business, or consumer confusion. Bona fide use, common usage and non-commercial or fair use may be exemptions from such liability.

---

248. The Rules for Uniform Domain Name Dispute Resolution Policy can be found at www.icann.org/udrp/udrp-rules-24oct99.htm (accessed 12.10.00). In addition, the ICANN-approved dispute resolution service providers have their own supplemental rules. The WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy can be found at http://arbiter.wipo.int/domains/rules-supplemental.html (accessed 12.10.00). The Supplemental Rules outline the formal requirements that the complaint and response must satisfy.
249. In practice, WIPO try to appoint panellists with the same geographic and judicial background as the complainant and the respondent. For example, in a case between a Danish complainant and a Norwegian respondent, WIPO appointed a Swedish sole panellist, see the «Welltractor case», http://arbiter.wipo.int/domains/decisions/html/d2000-1145.html (accessed 20.11.00).
250. Paragraph 4(c) of the Uniform Policy.
The following circumstances are deemed evidence of the registration and use of a domain name in bad faith:

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

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

3. you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

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

Examples of cases in which the domain name was registered primarily for the purpose of selling it to the complainant, or complainant’s competitor, for a greater amount than out-of-pocket expenses are: «bbcdelondres.com», «piper.com», «pharmore.com».²⁵¹

Examples of cases in which the domain name was registered in order to prevent complainant from reflecting the mark in a corresponding domain name, provided that the registrant has engaged in a pattern of such conduct are: «wwwreuters.com»²⁵² and «pharmore.com».

Examples of cases in which the domain name was registered to attract Internet users to a web site for commercial gain are: «worldcup2002.com»²⁵³, «ingersoll-rand.net»²⁵⁴.

Another example of circumstances of bad faith registration and use is «telstra.org»²⁵⁵.

²⁵¹. See http://www.arbforum.com/domains/ (accessed 27.11.00).
6.2.5 How to demonstrate rights to and legitimate interests in the domain name in responding to a complaint

According to section 4(c) of the Policy, any of the following circumstances, shall demonstrate rights or legitimate interests to the domain name:

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

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

3. you are making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

Examples of cases in which the registrant had the prevailing right or legitimate interest in the domain name, comprises:

(i) Registrant used, or prepared to use, the domain name in connection with a bona fide offering of goods or services, before notice of dispute: «eautolamps.com»\(^{256}\), «allocation.com»\(^{257}\), «cartoys.net»;

(ii) Registrant has been commonly known by the domain name, even if no trademark or service mark rights has been acquired: «penguin.org»\(^{258}\), «sting.com»\(^{259}\);

(iii) Registrant is making a legitimate non-commercial or fair use of the domain name, without intent to tarnish the trademark or service mark: «worldcup2002.com»\(^{260}\), «csa-canada.com»\(^{261}\), «saint-gobain.net»\(^{262}\).

6.2.6 The Policy and the new gTLDs

Critics have argued that as a result of the Policy and the proposed seven new gTLDs\(^{263}\), the holder of a SLD in one gTLD (e.g. «springwater.com») may be

---

263. See chapter 2 above.
able to assert some right to the identical SLD under another gTLD (e.g. «springwater.biz»).

On one hand, the mere fact that one holds a domain name under one gTLD cannot lead to any rights in the identical SLD under another gTLD. One of the reasons for adopting additional gTLDs is to allow others to use some of the «good» names in the new gTLDs. Thus the point is to allow co-existence of identical or similar SLDs under different gTLDs similarly to the trademark system of different trademark classes.

However, if you do business under one 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 trademark and to use it in any other gTLD.

Moreover, infringement cases could appear similar to those appearing in traditional trademark cases, such as likelihood of confusion, due to the overlapping «classes» of gTLDs, for example .com and .biz.

In other words, in such occasions one can submit a complaint under the ICANN Policy, and if successful, one may be able to deny the SLD to anyone else in any other gTLD.

### 6.2.7 Fees

All fees charged by WIPO in connection with the dispute pursuant to the Policy shall be paid by the complainant, except in cases where the respondent elect to expand the Panel from one to three panellists, in which case all fees will be split evenly by both parties.\(^{264}\)

### 6.2.8 Remedies

The remedies available to a complainant pursuant to any proceeding before the Panel is limited to cancellation of the domain name or the transfer of the domain name registration to the complainant.\(^{265}\) Thus there are only three possible outcomes of the proceeding:

1. Status quo – the domain name holder (the respondent) keeps the domain name

2. Transfer – the domain name is transferred to the complainant

3. Cancellation – the domain name is cancelled and neither the domain name holder nor the complainant is eligible to hold the domain name

\(^{264}\) Paragraph 4 (g) of the Uniform Policy.

\(^{265}\) Paragraph 4 (i) of the Uniform Policy.
In other words, the Panel cannot award damages. In order for a complainant to claim damages, it must enter into an ordinary court procedure.

6.2.9 Availability of court proceedings

The mandatory administrative proceeding requirements does not prevent either party from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded.

In such an event, the complainant usually accepts a place of jurisdiction in the complaint. Commonly, one of the two countries involved – usually the domain name holder’s place of citizenship – is chosen. If only country is involved, that country is usually chosen as the place of jurisdiction.

6.2.10 Implementing the decision

If the Panel decides that the domain name registration should be cancelled or transferred, ICANN will wait ten business days after they are informed by WIPO of the Panel’s decision before implementing the decision. ICANN will then implement the decision unless they have received during the ten-business-day period official documentation, such as a copy of a complaint, file-stamped by the clerk of the court, that either party have commenced a lawsuit against the other party.

If ICANN receive such documentation within the ten-business-day period, ICANN will not implement the Panel’s decision, and ICANN will take no further action, until it receives:

1. evidence of a resolution between the parties;
2. evidence that the lawsuit has been dismissed or withdrawn; or
3. a copy of an order from such court dismissing the lawsuit or ordering that the party does not have the right to continue to use the domain name.

In other words, if the Panel order a transfer of the domain name to the complainant, the respondent may prolong the dispute and continue to hold the domain name by issuing a writ. In an ordinary lawsuit, and a possible appeal, it may take more than a year before the case is finally settled. However, the complainant has the option to request for a preliminary injunction, which may resolve the case without further delay.

---

266. Paragraph 4 (k) of the Uniform Policy.
6.3 Advantages and disadvantages of the ICANN system

One may raise the question whether the dispute resolution should be left to the courts altogether. Is there any need for alternative procedures for domain name disputes? On the one hand, recognising the increase of commercial activity on the Internet, a method 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. 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 ccTLDs 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. Thus the arbitration procedures for domain name disputes that the ICANN Policy provides for should be, as it currently is, limited to the international gTLDs and the ccTLDs that are open for all registrants.

The gTLDs are not country-related, and they are granted by registrars located in different countries. Thus the gTLDs have no country affiliation. However, 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, at least temporarily, «fill the gap». The ICANN arbitration procedure 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, ICANN arbitration may face difficulties regarding enforcement and compliance as a result of the incomplete national and international judicial authority. In theory, the ICANN Policy provides for direct implementation of the results of the dispute resolution. The ICANN arbitration awards will be enforced with global effect as the registrars are contractually bound to implement the decisions. Moreover, one single procedure for all gTLDs is a preferable solution. However, in practice, how can a decision be enforced with lacking national judicial authority?

If the losing party in an ICANN arbitration procedure submits the case to a national court, it is not clear how a decision of a single national 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 ICANN arbitration procedure, 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 trademark and all related «goodwill» which goes with it.

The advantages of the ICANN system are that it avoids monopolistic practices. The ICANN system removes the registrars from the domain name dispute resolution and provides an independent and international dispute resolution body. Further, the ICANN brings together private and public entities and organisations, international and national, and provides a system of Internet governance at the international level. The ICANN Policy 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 ICANN system are that it is uncertain whether the various ICANN proposals will be implemented and complied with by the whole Internet community. Moreover, it is unclear how arbitration awards under the ICANN Policy may be implemented, enforced and complied with. Finally, and perhaps most importantly, the dispute resolution body lacks judicial authority, thus the parties may still go to their national courts – hence multi-jurisdictional and cross-border litigation problems are still present.

This dilemma is one of many ICANN must cope with in the future.

6.4 Domain name cases

It is essential to illustrate the clash between domain names and trademarks and the ICANN Policy by examining some of the cases and decisions.

The WIPO Arbitration and Mediation Center decided the «Julia Roberts case» on 29.05.00. A private person had registered the domain name «juliaroberts.com», together with several other domain names identical to

267. 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 potential problems with the ICANN dispute resolution policy is that it provides the trademark owner with two options: invoke the 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 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 distressing reminder of the potential pitfalls in cross-border trademark disputes over domain names.
famous actors’ names. The domain name was posted for auction at the web site «eBay». The Administrative Panel concluded that the domain name should be transferred to Julia Roberts. The Panel found that the domain name was identical to and confusingly similar to the name «Julia Roberts», that the registrant had no rights or legitimate interest in the domain name and that the domain name was registered in bad faith.269

In the «TOEFL case» (16.03.00)270, the sole Panellist stated that the Policy is intended for abusive domain name registration only:

«The Uniform Domain Name Dispute Resolution Policy (the «Policy») (...) is addressed to resolving disputes concerning allegations of abusive domain name registration.

The subject matter scope of the administrative proceedings by which such disputes may be resolved is carefully circumscribed, reflecting a cautious approach to a novel form of dispute resolution that was designed to address a rapidly evolving technological environment. This approach was largely developed through the WIPO Internet Domain Name Process and reflects the balancing and synthesis of a wide range of perspectives regarding governance of the Internet environment. Administrative Panels established by authorised dispute resolution service providers should confine themselves to findings of fact that are necessary to rendering decisions within their limited subject matter jurisdiction.

A «domain name» is a human-friendly form of Internet address. The domain name shares characteristics with traditional forms of business identifiers, principally trademarks, service marks and trade names. The domain name differs from the trademark (and by analogy, the service mark). The trademark identifies the source of goods in commerce. The domain name does not generally appear on goods as an indication of source; rather, it may – but does not necessarily – identify a producer or supplier of goods by its location on the Internet. The domain name is closely related to a trade name that identifies a particular business. The

---


269. It is worth mentioning that the Panel stated that even though the name «Julia Roberts» was not a registered trademark, Julia Roberts had acquired trademark rights in the name as a common law trademark. However, when the artist «Sting» argued his case with the same line of reasoning as in the Julia Roberts case, the Panel stated that «Sting» was a generic name and thus did not transfer the domain name «sting.com» to the artist Sting.

trade name may be invoked, in appropriate circumstances, to prevent or redress unfair competition.

Because the holding of a valid trademark evidences a link between a sign or symbol on goods in commerce and a particular producer or supplier, the Policy establishes the holding of a valid trademark as a presumptive basis for redressing unfair competition in the registration and use of a domain name. However, the Policy recognises that parties other than the trademark holder may have legitimate interests in the use of its sign or symbol in a domain name. It distinguishes such legitimate interests from a set of circumstances which are likely to represent abuse of the trademark holder’s rights. It is only the "bad faith" registration and use of a domain name that is prohibited by the Policy.

In the «Bridget Jones case» (25.09.00), a private person had registered the domain name «bridgetjones.com» in order to use it as a fan site. In principle, this is legitimate non-commercial use\(^{271}\). However, the sole Panellist found that the domain name should be transferred to the author, Helen Fielding\(^{272}\). Firstly, the domain name (registered 08.10.98) was confusingly similar to Fielding’s trademark BRIDGET JONES (registered 28.10.97). Secondly, the domain name holder had no legitimate rights or interests in the domain name. The reasoning was as follows:

«In the abstract, the use of a domain name incorporating a trademarked literary name to establish a fan club might constitute legitimate non-commercial or fair use of that name. However, there are several factors that persuade the Panel that a finding of legitimate non-commercial or fair use of Complainant’s trademark is not warranted in this proceeding.

First, the Panel notes that while paragraph 4(c)(i) of the Policy refers to «preparations to use» a domain name in the context of offering goods or services, paragraph 4(c)(iii) refers only to the active «making» of a «legitimate non-commercial or fair use». The express language of the Policy indicates that its drafters intended to limit the circumstances in which legitimate non-commercial or fair use could successfully be claimed. Applying the express language of the Policy to Respondent’s claim of legitimate non-commercial or fair use, the Panel finds that Respondent is not

\(^{271}\) According to the ICANN/WIPO Policy, para. 4 (c) «you are making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue», demonstrates your rights or legitimate interests to the domain name.

\(^{272}\) The decision is published at http://arbiter.wipo.int/domains/decisions/html/d2000-1000.html (accessed 09.10.00).
"making" such legitimate non-commercial or fair use of Complainant's mark in the disputed domain name."

As the domain name was registered nearly two years ago, and has never been used, the Panellist found that the domain name holder was not actively "making" a "legitimate non-commercial or fair use". It is important to note that the domain name registration policy for .com, .net and .org does not require that the registered domain name must be used. Nevertheless, the Panellist found that there was no legitimate interest to block a domain name for two years. One may interpret this as an obligation to use a registered domain name or a doctrine of laches. Had the domain name holder in fact used the domain name as an active fan site, this might have constituted legitimate non-commercial use.

Thirdly, the Panellist found that the domain name had been registered in bad faith. The domain name holder had offered to sell the domain name to Helen Fielding at a substantial price (USD 15,000). The Panellist noted that "standing alone, an offer to sell a domain name in response to a demand from another party does not constitute bad faith within the meaning of the Policy". However, the domain name holder was aware of the commercial value of the trademark, thus it was reasonable to assume that he had registered the domain name with the intention to selling it to the trademark owner for a valuable consideration. This constituted bad faith.

In the "Madonna case" (12.10.00), the domain name "madonna.com" was registered by a private person. He was in the business of developing web sites and had purchased the registration for the disputed domain name for $20,000. This person also registered MADONNA as a trademark in Tunisia, and then he began operating an "adult entertainment portal web site". The complainant was the well-known artist Madonna. She is the owner of U.S. Trademark Registrations for the trademark MADONNA for entertainment services and related goods. She has used her name and trademark MADONNA professionally for entertainment services since 1979.

In this case, the Panel discussed the question regarding standard of proof in domain name disputes:

"A threshold question in proceedings under the Policy is to identify the proper standard for reaching a decision on each of these issues (...)"

Although the nature of the record is similar to that found on a summary judgment motion, our role is different than that of the Court on a sum-

mary judgment motion. Paragraph 15 of the Rules states that the "Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy. . ." Paragraph 10 of the Rules provides that the "Panel shall determine the admissibility, relevance, materiality and weight of the evidence." Paragraph 4 of the Policy makes repeated reference to the Panel’s role in making findings of fact based on the evidence.

Based on the Policy and the Rules, we disagree with the view that disputes over material facts should not be decided in these proceedings. Rather, it is clear to us that our role is to make findings of fact as best we can based on the evidence presented provided the matters at issue are within the scope of the Policy. There may be circumstances due to the inherent limitations of the dispute resolution process or for other reasons where it would be appropriate for a panel to decline to decide a factual dispute. However, the mere existence of a genuine dispute of material fact should not preclude a panel from weighing the evidence before it and reaching a decision.

Since these proceedings are civil, rather than criminal, in nature, we believe the appropriate standard for fact finding is the civil standard of a preponderance of the evidence (and not the higher standard of "clear and convincing evidence" or "evidence beyond a reasonable doubt"). Under the "preponderance of the evidence" standard a fact is proved for the purpose of reaching a decision when it appears more likely than not to be true based on the evidence. We recognize that other standards may be employed in other jurisdictions.

The Panel found that the disputed domain name was identical or confusingly similar to a trademark in which the complainant had rights, the respondent lacked rights or legitimate interests in the domain name, and the domain name had been registered and used in bad faith. Therefore, the Panel decided that the disputed domain name «madonna.com» should be transferred to the complainant.

Of the «Norwegian» domain name cases that have appeared before the WIPO, is «forbrukerraadet.com», «legeforeningen.com» and «skatteetaten.com», the most famous ones.274

In the case regarding legeforeningen.com, the Panel decided that Eivind Nag, and not Den norske lægeforening, should hold the domain name:

Complainant has failed, on this record, to establish trademark rights in the designation «legeforeningen.com». Accordingly, Complainant has failed to satisfy Paragraph 4 (a) (i) of the Policy. The Panel therefore denies the Complainant’s request that the domain name «legeforeningen.com» be transferred from Respondent to Complainant.

In the case regarding skatteetaten.com, the Panel decided that the domain name should be transferred to the complainant – skatte-etaten. The Panel stated that:

The Complainant has used, since many years, the term "Skatte-etaten" as a business identifier and the Panel is satisfied that the Complainant has rights in that business identifier. However, under the Policy, the Complainant must have rights in a mark (trademark or service mark). The Complainant has no registration of the word "Skatteetaten" as a mark. However, Norwegian Trademark Law also recognizes rights on unregistered marks on the condition that they have acquired distinctiveness through use (…)

The Respondent claims that he intended to use the domain name in issue to satirize the Complainant. The Panel accepts that it is, in principle, legitimate to operate a domain name for the purposes of lawful criticism of a trademark owner. The Panel does not, however, believe that this right extends to occupying a domain name identical to a sign identifying a trademark owner. In particular, the Panel believes that anyone wishing to contact a trademark owner, has the right to contact the owner by addressing himself to the owner’s exact identifier, followed by the top level suffix, in this case .com, and to thereby reach the trademark owner, and not a third party, which itself does not have rights in that mark (…)

For a Complainant to succeed, not only must the Panel be satisfied that a domain name has been registered in bad faith, but must also be used in bad faith. As an example, the Policy section 4(b) (i) mentions registration or acquisition of the "domain name primarily for the purpose of selling....". The general test is therefore whether a Respondent has attempted to sell the domain name for a sum in excess of the Respondent’s out of pocket expenses in registering the domain name. In this case, the Respondent wrote to the Complainant on August 9, 2000:

"The domain names have been an expense for us, and we will rather not keep the domain names. To cover our expenses and work we are planning
to sell the domain names to market price. If you are interested, we will give you priority to buy them" (...) 

Furthermore, the Respondent, in his subsequent telephone conversation with the Complainant, according to his own statement in the Response, went on to say: "You have a week from now to decide if you want to buy it back, after which I will sell it for "market price" to the highest bidder". This, in the Panel’s opinion, is a strong evidence of bad faith (...) 

The Panel, accordingly, decides that the Complainant has proven each of the three elements of paragraph 4a of the Policy, and requires that the registration of the domain name "skatteetaten.com" be transferred to the Complainant.

In the «Telstra case» (18.02.00), the domain name «telstra.org» was registered by Nuclear Marshmallows.275 It was held in the Telstra case that the domain name telstra.org should be transferred to the complainant Telstra based upon the following facts:

1. «the Complainant’s trademark has a strong reputation and is widely known, as evidenced by its substantial use in Australia and in other countries,

2. the Respondent has provided no evidence whatsoever of any actual or contemplated good faith use by it of the domain name,

3. the Respondent has taken active steps to conceal its true identity, by operating under a name that is not a registered business name,

4. the Respondent has actively provided, and failed to correct, false contact details, in breach of its registration agreement, and

5. taking into account all of the above, it is not possible to conceive of any plausible actual or contemplated active use of the domain name by the Respondent that would not be illegitimate, such as by being a passing off, an infringement of consumer protection legislation, or an infringement of the Complainant’s rights under trademark law.»

The Panellist also stated that «the significance of the distinction is that the concept of a domain name «being used in bad faith» is not limited to positive action; inaction is within the concept. That is to say, it is possible, in certain circumstances, for inactivity by the Respondent to amount to the domain

name being used in bad faith». The Panellist posits that:

«the question that then arises is what circumstances of inaction (passive holding) other than those identified in paragraphs 4(b)(i), (ii) and (iii) can constitute a domain name being used in bad faith? This question cannot be answered in the abstract; the question can only be answered in respect of the particular facts of a specific case. That is to say, in considering whether the passive holding of a domain name, following a bad faith registration of it, satisfies the requirements of paragraph 4(a)(iii), the Administrative Panel must give close attention to all the circumstances of the Respondent’s behaviour. A remedy can be obtained under the Uniform Policy only if those circumstances show that the Respondent’s passive holding amounts to acting in bad faith.»

A case that can be compared to that of Telstra is the «Allocation case» (24.03.00),276 which adopted a different rationale and hence provided a different outcome. The respondent in this case operated a web site under the domain name «rockbottomdomains.com» where he offered for sale «allocation.com» as well as a number of other domain names many of which may also give rise to action from registered trademark owners. The complainant had registered the domain names «allocation.net», «allocation.org» and «allocation.de».

The Panellist stated that:

«the fact that, as Complainant has shown, a number of other domain names registered by Respondent are identical to different national trademarks from different owners is in itself insufficient evidence of the intent to profit from or otherwise abuse such trademark rights. After all, this is to be expected, in view of the territorial nature of trademark rights and the fact that, as set out above, terms which are descriptive or generic for particular goods or services and/or in a particular country may be considered valid trademarks for other goods and services and/or in a country with a different language.»

The cases represent two extremes. In the Telstra case, the Panel allows the trademark owner the right to exercise an international monopoly and exclusive use over the registered trademark. In the Allocation case, the Panel found that:

«nothing in the Policy can be construed as requiring a person registering a domain name to carry out a prior trademark search in every country of

---

the world for conflicting trademark rights, as advocated by Complainant. Since it is therefore not demonstrated that Respondent at the time of registration of the domain name allocation.com knew or should have known of the existence of the German trademark Allocation, there is no evidence suggesting that the domain name allocation.com has been chosen by Respondent with the intent to profit or otherwise abuse Complainant’s trademark rights.»

This decision grants the domain name holder the right to exploit the commercial value that the Allocation trademark has attained. Essentially what is needed is the balancing of these two decisions whereby the rights of trademark owners are protected, but do not give rise to a monopolistic protection over the trademark. The difficulty with this is distinguishing when the domain name holder is undertaking a legitimate entrepreneurial venture and those actions which go one step further and may be deemed to be cybersquatting.

There is a clear tendency in the ICANN cases to protect the trademark owner. In the «Welltractor case» (31.10.00), the domain name «welltractor.com» was registered by one of the chief executives in the division of the Norwegian company Aker Maritime called Maritime Well Service («MWS»). MWS produces, among other products; well tractors called «Power Trac» for the oil and gas industry. The complainant, the Danish company Welltec, has developed and manufactured a well tractor called «Well Tractors» and had registered the trademark WELL TRACTORS.

It was held that the domain name «welltractor.com» should be transferred to the complainant. The complainant alleged that «after all applicable standards of trademark law the domain name welltractor.com must be considered confusingly similar to the trademark Well Tractors». The respondent replied that «the term «well tractor» is a generic word and Complainant must tolerate that other entities make use of the term. It is not confusing the relevant customers that the domain name and the trademark co-exist. The term is a descriptive word generally and widely used as the term for the product in this particular business sector».

Furthermore, the respondent alleged that it had rights and legitimate interests in respect of the domain name. The domain name was registered and used in good faith as the domain name welltractor.com was registered simply because MWS produces and manufactures well tractors. Respondent alleged that the complainant could not by trademark registration obtain monopoly.

on the use of a descriptive term. Otherwise, this would undermine the whole concept of the first come first served principle in domain name registration.

Nevertheless, the panellist found that the domain name should be transferred to the trademark owner. As regards the registration of a generic term, the panellist stated that:

«The Respondent’s allegation that the words "well tractor" constitutes a generic name cannot be taken into account in this Administrative Proceeding for the following reasons. The trademark WELL TRACTORS is a registered trademark in Norway and in an English speaking region and country namely the European Community and the US. In the trademark laws of this region and country, trademarks are examined with respect to distinctiveness and there are absolute grounds for refusal of generic words. The US-Registration contains a disclaimer but only for the word "well" itself. Consequently, these trademark registrations constitute prima facie evidence of distinctiveness. In order for genericness to be taken into account in an Administrative Proceeding it would be necessary to present convincing evidence showing that the words "well tractors" were obviously generic at the time of the registration or that they have thereafter become generic through degeneration. Such evidence has not been presented by the Respondent and can only in obvious cases be considered prejudicially in a written administrative procedure. However, this decision should not be interpreted as a final decision stating that Complainant’s mark is generic or not.»

This decision illustrates a tendency – «the trademark owner gets it all» – and many critics allege that the system has gone astray. Another problem is that should a trademark owner lose in an ICANN process, he can go to court to protect his trademark and is likely to obtain the domain name. On the other hand, if the domain name owner loses in the ICANN process, it has proven to be very difficult to go to court and keep the domain name. Interestingly, in a recent case in Florida, the court went against the ICANN decision and re-allocated the domain name to the domain name holder.278

---

278. The decision was passed in November 2000. Unfortunately, I have not found the correct case citation.
7. INTERNATIONAL GOVERNANCE OF THE INTERNET

Aims of chapter 7
The aims of Chapter 7 are to:

• outline the problems the trans-national 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

• evaluate the ICANN system as a case study.

The current domain name system is described in detail in the previous sections of this book. Without a satisfactory 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 and how one can prevent intellectual property infringement.

This chapter argues that what the Internet needs, is an agreed system of governance that is truly representative, responsible and accountable. Our current national legal framework is designed for a world of barriers and distance. However, the Internet transcends 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. Thus current domestic law does not adequately resolve all the problems and challenges the Internet poses. In order to maintain public confidence in any system of domain name allocation and domain name dispute resolution, 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 outlined above.

279. Selin, S., «Governing Cyberspace: The Need for an International Solution» (1996/97) 32 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 co-ordinated, 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 key point is, however, that the Internet «tends to ignore national boundaries and previous treaties have not adequately envisioned this medium». See Selin at pages 379 and 380.
7.1 The Internet creates challenges 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 trans-national, border-less and multi-jurisdictional. The world-wide network of computers is not within the territorial jurisdiction of any sovereign. Some theorists have stated that «national borders are just speed-bumps on the information superhighway». What is certain is that 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 the 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 are 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 one single government cannot enforce rules on an Internet-wide basis.

This lead to another problem domestic legal systems has experienced when endeavouring to deal with Internet activities. What factors are relevant in order to establish jurisdiction over the national portion of the Internet? For example, will mere accessibility of a web site in a territory be sufficient to

---

280. Quoted in Selin, at page 366.
282. 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, at 372.
establish jurisdiction in that territory over the entity that owns or controls the web 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. Due to the trans-national nature of the Internet, in many cases there will not be the relevant nexus with the state (e.g. Norway) in which the trademark holder can sue. If an alleged breach occurs on the Internet and all that connects that breach to Norway is a passive web site, then it is doubtful whether the courts would exercise exorbitant jurisdiction. Indeed, the US courts have already found it difficult to identify what creates a sufficient nexus to give jurisdiction.

As regards marketing in the Nordic countries, the consumer ombudsmen in the Nordic region have issued a joint paper regarding their approach towards marketing on the Internet and under which jurisdiction such Internet activity falls within the area of responsibility. According to that paper, the relevant question is whether the marketing is targeted towards that jurisdiction. In order to consider whether, due to an overall evaluation of the marketing, Norwegian jurisdiction applies, the following factors can be used as indicators:

---

283. Some decisions, for example The Playboy Enterprises Inc. v Chuckleberry Publishing 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 absence of anything else, the site was directed to persons in New York such as to give the courts of New York jurisdiction. See also «Current Developments» «No Personal Jurisdiction over Out-of-State Web Page Owner» (1996) 13 (9) The Computer Lawyer 24 at 24.

The reason why the American theorists divide the jurisdiction into personal jurisdiction and subject-matter jurisdiction, 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 jurisdiction are rarely disputed. Personal jurisdiction, however, is more complex. Personal jurisdiction is the power to make the wrongdoer obey its orders.

284. Selin, at page 371.

285. Note that the Internet service providers (ISPs) are neither administrators 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, according to Selin, 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». See Selin, at 374.

286. See O11r1(2) Supreme Court of Qld Act 1991.
• which language, currency or other national characteristics are used;
• to which extent the business or service is generally marketed in the relevant jurisdiction;
• whether there is a link or connection between the marketing on the Internet and other marketing efforts in the relevant jurisdiction; and
• whether the business accepts contracts or other transactions with customers domiciled in the relevant jurisdiction.

Other problems arising for domestic legal authorities regarding the Internet are issues such as the lack of standards for evidence collection, the problem with the wide use of anonymous re-mailers, censorship, criminal law issues and human rights issues. These issues will not be addressed in this book.²⁸⁹

²⁸⁷. 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), 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.


²⁸⁹. For more details regarding jurisdiction and the Internet, see Andreas Frølich Fuglesang and Georg Philip Krog, «Internett og jurisdiksjon», Complex 3/99.
7.2 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 work perfectly 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 ICANN system is the most feasible solution and whether the Internet would merit from a system of trans-governmental governance.

There are four basic competing models for governance of the Internet:²⁹⁰

- 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 community;
- International treaties. Sovereigns may enter into multilateral international agreements to establish uniform rules applicable to conduct on the Internet;
- 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 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.²⁹¹ 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

---
²⁹¹ Selin, at 366. As discussed above, state governance of the Internet is not feasible.
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.²⁹²

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 an international agreement on domain names.²⁹³ 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.²⁹⁴ Any authority will only be globally authoritative if every national sovereign accepts its decrees. However, this would, according to international law theorist Margaret Jane Radin, require a full-scale network of treaties.²⁹⁵ One could also imagine a piecemeal process of treaty-making, issue by issue. How-

²⁹². See Selin, at page 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.

²⁹³. 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?.

²⁹⁴. Johnson and Post, «And How Shall the Net Be Governed?». 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.

²⁹⁵. See also Johnson and Post, 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.
ever, as Slaughter points out, this kind of world government, even as an ideal, is unfeasible at best and dangerous at worst.\footnote{Slaughter, at page 1.} 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». This book 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.

Several Internet users see self-regulation as an attractive possibility, primarily because it is seen as offering a realm of free choice.\footnote{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, at page 378. See Tarjanne, P. «The ITU Responds to New Concepts for Public Policy in the Global Information Society» (1992) 13 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.} Internet users would like to consider the Internet as its own 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.\footnote{Johnson and Post, «And How Shall the Net Be Governed?». 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».} 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 than planning. In other words, they are thinking about a regulation which is not laid down, but grown up.\footnote{See Radin.}

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.\footnote{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?».} Post also suggests that the enforcement mechanisms could be laid down by the «sys-ops».\footnote{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.  

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». In other words, Post suggests that the Internet should continue its informal system of self-regulation. 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 conditions have also been criticised because they are imposed on would-be residents on a «take-it-or-leave-it» basis. 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.\(^{309}\) 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».\(^{310}\) This book 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 international organisation does not need to obtain the agreement of all interested governments.\(^{311}\) Hence an international organisation may attempt to establish and enforce basic rules for the Internet. Up until 1999, voluntary, private persons and entities ran the Internet.\(^{312}\) Today the ICANN is an example of international organisations, private and public entities providing an international Internet governance institution with authority to lay down rules about domain name allocation and dispute resolution.\(^{313}\) ICANN has been recognised by the U.S. Government as the global consensus entity to co-ordinate the technical management of the Internet’s domain name system, the allocation of IP address space, the assignment of protocol parameters, and the man-

---

309. See also Johnson and Post, «And How Shall the Net Be Governed?». 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.

310. 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 harsh 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.

311. See Johnson and Post, «And How Shall the Net Be Governed?».
agement of the root server system. However, ICANN’s mandate is not to «run the Internet». Rather, it is to co-ordinate the management of only the specific technical, managerial and policy development tasks that require central co-ordination – the assignment of globally unique names, addresses, and protocol parameters. According to ICANN’s web page, ICANN is «dedicated to preserve the operational stability of the Internet; to promote competition; to achieve broad representation of the global Internet community; and to co-ordinate policy through private-sector, bottom-up, consensus-based means».  

Furthermore, according to ICANN itself, it «represents a unprecedented effort by the Internet business, technical, non-commercial and academic communities to create a globally representative private sector (that is, non-governmental) policymaking body. Consistent with the principle of maximum self-regulation in the high-tech economy, ICANN is perhaps the foremost example

312. 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, can not 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?». The US government has 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».  

313. It has not always been clear who has the ultimate authority to grant and revoke a domain name. For example, the IANA, who has played an important role in the stability of the Internet, where did it get its authority? For information about the IANA and its role, see Chapter 1 «The main Internet players» above. According to the IANA web page, the IANA «is chartered by the Internet Society and the Federal Network Council». Hence the next question is where did the Internet Society and the Federal Network Council (FNC) get their authority? The FNC is chartered by National Science and Technology Council’s Committee on Information and Communications (CIC). 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 Sub-committees 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, which have been and currently are involved in the Internet governance and administration.

of collaboration by the various constituents of the Internet community – individuals and organisations, entrepreneurs and educators, corporate enterprises and non-profit advocacy groups. Though often contentious, the ICANN structure creates an open and transparent global forum in which competing interests can work toward consensus.315

7.2.1 International organisations

As the Internet is a global resource the allocation of domain names is a global issue. 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 is an international 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.

Yet another obstacle is how a non-governmental organisation can impose its rules on the Internet as a whole. Further, even if ICANN controls the current DNS, how can 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 ICANN’s strongest asset is the numerous international organisations, private and public entities which are members to it. The endorsements of the ICANN 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 members makes the ICANN representative. Hence it will gain a reputation and authority no single international organisation will ever be able to assemble. In other words, the endorsements of the ICANN may amount to the «rough consensus» that the Internet community tends to follow. Therefore, the ICANN assembling the relevant international organisations may transform international organisations to feasible instruments for Internet governance.

315. See http://www.icann.org/general/background.htm (accessed 04.12.00).
7.2.2 Should the state remain the key international player?

The mixture of international, public and private entities supporting the ICANN thus creates a trans-governmental 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 trans-governmental 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 trans-national governance to usurp international governance.\(^{316}\)

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 sub-national counterparts, creating the potential for truly global government networks».\(^{317}\) The hallmark of trans-governmentalism, 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.\(^{318}\) 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 trans-governmental 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.\(^{319}\) However, this leads to the

---

\(^{316}\) Slaughter, at page 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.

\(^{317}\) Slaughter, at page 6.

\(^{318}\) Slaughter, at page 18.

\(^{319}\) In contrast to Radin’s view, 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, at 1.
issue of what kind of governance the ICANN establishes. The question is how the ICANN system fits in with Slaughter’s view. The ICANN is an example of international institutions, such as WIPO, and key trans-national Internet actors, such as ISOC and IANA, agreeing to form a governance structure implemented through several regional allocation registries. The ICANN preserves the original idea of self-government and provides for a compromise solution.\footnote{The ICANN Policy does not require any state involvement, except for the national courts as the last resort in the domain name dispute resolution procedure. The Policy uses principles of self-governance, sets up a structure and establishes policies and procedures, for responsible administration of the «generic» portion of Internet domain name space.} The administrative structure of the ICANN also includes interference of state governments. In other words, it does adopt Slaughter’s suggestion to obtain power and authority from the state institutions. Furthermore, the ICANN establishes a centralised decision-making institution. It is a hybrid of commercial entities and international, public and private organisations. In many ways, the ICANN may be categorised as the commercial sector’s attempt to manage the Internet. As a result of the commercial sector having no enforcement power, there is a need for the state institutions for enforcement and compliance purposes. The ICANN draws on the authority of such public governments and state institutions.

The ICANN establishes 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 ICANN establishes a fairly 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.

One alternative 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 other words, international and municipal law would support a new theory – one which is capable of devolv-
ing power and decision among various international, public and private enti-
ties. State institutions should co-ordinate and co-operate in order to
courage Internet governance by trans-governmental institutions.

In conclusion, international organisations are suited to set Internet policy. The ICANN, where state governments and trans-governmental organisations world-wide are creating an international domain name organisation, is a wel-
come and interesting development. However, the state institutions should pro-
vide the necessary authority and power to make trans-governmentalism a workable solution. This book will argue that international organisation can not realistically govern the Internet without the power of state institutions. Thus a new theory for Internet governance, where trans-governmental institu-
tions 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.321

321. Slaughter, 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 abso-
lute power in domestic affairs and autonomy in relations with other states». See Slaughter at 28.
8. **DOMAIN NAME REGISTRATION IN NORWAY**

8.1 **Introduction**

Norway was in fact the first country outside the US that got access to the Internet (ARPAnet). It happened in 1973 as a part of the Defence political cooperation between the US and Norway.

In Norway, the domain name allocation is administered by NORID (NOrsk Registreringstjeneste for Internett Domenenavn). In order to obtain a registration under the domain name «.no» from Norid, the applicant must be an entity registered with the Norwegian Registry of Business Enterprises. In practise, an organisation number demonstrates this.

Today, an organisation may register 15 domain names. A so-called registrar carries out the registration of a domain name. Currently, there are more than 300 registrars approved by Norid.

8.2 **The domain name policy**

Norwegian domain name policy has been restrictive, especially if one compares with the policy for «.com».

Domain names are allocated on a first come, first served basis. The applicant must have a Norwegian organisation number. In other words, private

---

322. NORID is a part of the organisation UNINETT AS, which administers the domain name «.no». UNINETT AS is a neutral and non-commercial entity 100 % owned by the Ministry of Church, Education and Research (KUF). Information regarding UNINETT can be found at www.uninett.no. NORID works openly towards the Norwegian Post and Telecom Authority (PT), however there are no formal rules of co-operation between them. For information regarding NORID, visit www.norid.no. The Norwegian Post and Telecom Authority (NPT) has recommended that the co-operation between NPT and Norid should be subject to contract, based on the proposal «Principles for the Delegation and Administration of Country Code Top Level Domains» from GAC. For more details on NPT’s proposal, see http://www.npt.no/norsk/fagomraader/off_telenett/dokumenter/domenenavn.html (accessed 31.10.00).

323. The Norwegian domain name policy is available at www.norid.no/navnepolitikk.html.

324. In order to become a registrar one must enter into an agreement with Norid. For more information, see http://www.norid.no/registrarside.html (accessed 31.10.00). The standard registrar agreement can be viewed at http://www.norid.no/registrar/regavtale.html (accessed 31.10.00).

325. The Norwegian domain name policy paragraph 2.2
persons and foreign entities are omitted. Individuals may register a third-level domain name under the domain name space «priv.no».

The domain name must consist of 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. Thus, the opportunity to use its trademark and other service marks as a domain name has been restricted. The policy states that as a general rule, a trademark, product name or other designation cannot be registered as a domain name. However, exceptions can be made if the organisation is only known under the trademark or product name and not its own name.

Upon registration, the organisation must sign a statement in which it warrants that to its knowledge, the domain name does not infringe upon or otherwise violate the rights of any third party. Norid does not make any preliminary inquiry or investigation.

By way of getting round this strict policy, entities have incorporated dormant unlimited liability companies that each has been granted one domain name. This is clearly not a satisfactory situation.

8.3 The new policy

The domain name policy has recently been amended. The first amendment entered into force 04.05.00. As a consequence, an organisation can now register a generic or descriptive word as its domain name. Furthermore, acronyms, names and abbreviations are allowed.

Accordingly, an entity may now register the descriptive term «milk» as a domain name. However, currently there is still a requirement that there is a link between the organisation and the domain name. This means that in order to register «milk.no», the organisation, its products or the object of the company must have a sufficient nexus with dairy products. Nevertheless, the policy does not clearly stipulate the required link.

The second amendment implemented the rule that one organisation is allowed to register 15 domain names. Furthermore, the link requirement between the organisation and the desired domain name will be abolished.

326. EUnet Norge administers the name space «priv.no». The name policy is available at http://193.71.71.193/navn/politikk.html (accessed 12.10.00).
327. The Norwegian domain name policy paragraph 4.2.
328. The Norwegian domain name policy paragraph 5.2.
Thus, an entity may register domain names corresponding with its trademarks, product names, projects and campaigns. Norid shall not perform any preliminary search prior to registration. Furthermore, there will be no mechanisms for domain name dispute resolution.\(^{330}\) Instead, the statement in which the applicant warrants that to its knowledge, the domain name does not infringe upon or otherwise violate the rights of any third party will be retained.\(^{331}\) Also, the requirement to show an organisation number will be retained.

### 8.4 The risk of conflicts

The new policy clearly acknowledges the domain name’s hallmark and function as a «trademark» on the Internet. This makes it easier for an entity to utilise Internet as a medium for marketing of its goods and services – without evading the law. Thus an entity may efficiently incorporate its domain names in a joint marketing and trademark strategy. The marketing value of a good, easy and catchy domain name, in combination with trademarks in the tangible media, may be considerable.

The risk of conflicts between the traditional trademark in the real world and a domain name in cyberspace emphasises the importance of documenting its right to use a domain name. It is not clarified in Norwegian practice whether a domain name in general gives grounds to challenge a younger company name or trademark. With a similar company name and/or a trademark registration, the company’s possibilities in a potential lawsuit regarding its domain name is strengthened. A domain name alone is not as strong should a proprietor of older company name or trademark allege that the domain name infringes upon its rights.

The new policy leads to a smoother, more efficient and cheaper way of registering several domain names. This will facilitate more customer friendly and

\(^{330}\) Norid and the Norwegian Post and Telecom Authority has recommended to temporarily postpone the establishment of a dispute resolution organ. WIPO is currently working on a report on dispute resolution for ccTLDs. On November 6th and 7th there is a WIPO International Conference on Dispute Resolution in Electronic Commerce. The conference is organised by the WIPO Arbitration and Mediation Center in co-operation with the London Court of International Arbitration (LCIA), the Dispute Resolution Section of the American Bar Association (ABA), the Singapore Subordinate Courts and the Swiss Arbitration Association (ASA).

\(^{331}\) Before signing the statement, one should make some preliminary inquiries or investigation. For example, one may search the Norwegian Registry of Business Enterprises for identical or similar company names, see www.brreg.no. The Norwegian Patent Office should be contacted in order to search for identical or similar trademarks. The Patent Office performs search in order to identify similar marks that are likely to infringe or cause a likelihood of confusion. Such search must be ordered in writing and is usually performed within 1-4 days.
fanciful domain names and the Internet’s basis as a means for marketing and sale is strengthened. However, this might result in further disputes regarding confusingly similar domain names and trademarks, domain name piracy and sale of domain names for commercial benefit. This may lead to a «registration hysteria» and more unnecessary registrations for safety reasons. This author’s impression, however, is that most people are willing to accept this risk in order to achieve increased freedom of choice when registering a domain name.

9. SOME FINAL REMARKS

The Internet has been in a process of transition. Some years ago, large business enterprises were found to be asleep at the wheel on the information superhighway. Today, they are awake and aware of the challenges and possibilities the Internet poses.

Robert Shaw, advisor of the International Telecommunication Union (ITU), illustrates this 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».*

333

Up until now, if the domain name one desired were already assigned, the options have been to register for a different name, pay the resale price, sue, or register the name one requested in a different TLD. With this background in mind, the ICANN shared registration system and dispute resolution mechanisms proposes a feasible and desirable solution. It includes Internet stakeholders in the governance of the Internet, preserves the idea of self-governance, suggests more gTLDs, provides resolution of the conflicts between domain names and trademarks, and implements the solution on a much larger scale than the previous proposals. In other words, the ICANN attempts to create a stable environment for commerce on the Internet.

What is more important, is that ICANN, unlike its predecessors, have included public authority representatives from governments all over the world in its GAC. Although there are no sovereign governments that are signatories to it, it has obtained the transgovernmental authority required to cope with the difficulties with getting all countries to respect, implement, enforce and comply with ICANN’s decisions and proposals.

If the ICANN/WIPO decisions regarding domain name disputes are successfully implemented and the suggested new gTLDs are added to the root servers, the new system is likely to work and the regulation of domain names will improve. Over time, as the new gTLDs acquire reputation and entities start registering in them, the new domain names are likely to dilute the popular «.com» and the domain name system is likely to become «trademark-like».

---

333. Shaw, «Internet Domain Names: Whose Domain Is This?». 
As a temporary solution, the best approach would be to leave the domain name disputes to the local courts. The Norid «hands-off» approach is an example of workable a policy for domain name allocation and dispute resolution which are currently being utilised. In the long term, however, transgovernmentalism should prevail. 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. The state will provide legitimacy as the Internet players need a more enhanced legitimacy than the system the Internet currently previously worked on – «rough consensus». Therefore, transgovernmental organisations, states and international and supra-national institutions should co-operate to solve the current and forthcoming obstacles.

The present-day emphasis on domain names seems to be at a peak. In coming years search engines, «whois» directories and other meta layers of Internet interaction will develop that might make domain names less important and thus not worth fighting over. 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. 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, are now viewed as relevant. The Internet is in an important stage of its life and needs just a little more 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.
APPENDIX 1
DOMAIN NAME ALLOCATION POLICIES
AND THE LOCAL COMPANY REQUIREMENT
IN EUROPE

1. Background
As each country governs its own ccTLD, there are various domain name poli-
cies throughout Europe. ICANN gives general directions regarding the gov-
ernment of the ccTLD, e.g. that the ccTLD should favour the users’ interests
in the relevant region the ccTLD applies to. However, ICANN does not give
any specific directions on the administration and handling of the ccTLD.334

In many countries, there is a business presence requirement in order to reg-
ister a domain name under the ccTLD. Consequently, one needs a local com-
pany in order to obtain a domain name under the ccTLD.

2. Establishment of companies
Many of the European domain name policies require a local company pres-
ence. This applies, inter alia, to Norway, Sweden, Germany, France, Portugal
and Spain.

In such case, it is recommendable to establish a private limited liability
company. Unexpected consequences may follow an unlimited liability com-
pany in a foreign jurisdiction. The downside with limited liability companies,
however, is the share capital requirements that will tie up fairly large amounts
of capital. If possible, one should establish a local division of its company, as
this usually does not require share capital or have a lower share capital
requirement.

3. Trademark registration
In some countries, a national trademark registration is sufficient in order to
obtain a domain name registration. This applies, inter alia, to Belgium, Italy
and Finland.

334. See «Principles for Delegation and Administration of ccTLDs Presented by Governmental
Advisory Committee», at www.icann.org/gac/gac-cctldprinciples-23feb00.htm (accessed
31.10.00).
If one has applied for a Belgian trademark registration, one may obtain a temporary (usually six months) domain name registration. When the trademark is registered, the domain name registration becomes final upon showing the trademark registration certificate.

4. Unrestricted domain name allocation
In some countries, the domain name allocation is unrestricted. This applies, inter alia, to Luxembourg, Switzerland, Austria, the UK and Denmark.

5. Domain name registration in some European countries – a non exhaustive list

Norway «.no»

Local company requirement:
In Norway, a company may register 15 domain names. It is common to register unlimited liability companies, as there is no share capital requirements. After registering the companies with the Norwegian Registry of Business Enterprises, one may register domain name(s).

Costs amounts to approximately NOK 5,000 to the Registry of Business Enterprises, legal fees (approximately NOK 5,000), plus fees to auditor. In addition, there are potential costs regarding trademark registration.

Domain name registration:
Domain names may be registered upon showing an organisation number. Costs are a one-time fee of NOK 450 and a yearly fee of NOK 100.

Sweden «.se»

Local company requirement:
In Sweden, one must establish as many limited liability companies as the number of domain names one wishes to register. The share capital requirement is SEK 100,000. It is possible to buy shelf companies for this purpose, at a cost of approximately SEK 9,000 (including registration) per company. After buying the shelf company, it takes one week to change the company name.

In addition, there are potential costs regarding trademark registration.

335. See www.norid.no
336. See http://www.nic-se.se/
Domain name registration:
Domain names may be registered when the company name is changed and registered with the Swedish Patent- and Registration Authority (PRV). One is entitled to one domain name per organisation. The domain name must correspond with the company name. Registration of a domain name usually takes two days.

The Swedish domain name rules are under amendment.337

Denmark «.dk»338

No local company requirement:
In Denmark, there is no company requirement to register a domain name.

Domain name registration:
Any legal or physical person may register domain names. Costs are DKK 150 in registration fee and DKK 40 in yearly fee. Registration of a domain name usually takes two days.

Finland «.fi»339

Local company requirement:
In Finland, professionals and entrepreneurs registered with the Finnish Trade Register may apply for domain names under «.fi». It is a share capital requirement of Euro 8.000. It is possible to buy shelf companies for this purpose, at a cost of approximately FIM 60.000 (including registration and share capital) per company. After buying the shelf company, it takes one week to change the company name.

In addition, there are potential costs regarding trademark registration.

Domain name registration:
A legal entity registered in Finland is entitled to several domain names. Such entity may also apply for domain names based on its registered Finnish trademark or EU trademark. However, a legal entity registered in Finland cannot be granted a domain name based on its international trademark registration under the Madrid protocol. Registration of a domain name usually takes ten days. Costs are FIM 320 in registration fee and FIM 60 in yearly fee.

337. The amendments are expected to be implemented on 31.12.2000. For details, see SOU 2000:30.
338. See http://www.dk-hostmaster.dk/
339. See http://www.thk.fi/
Germany «.de»

Local company requirement:
In Germany, one must establish a limited liability company. The share capital requirement for a GmbH is DM 50,000 and for an AG is DM 100,000.

In addition, there are potential costs regarding trademark registration.

Domain name registration:
The company must sign a statement warranting that to its knowledge the domain name does not infringe upon any third party’s rights. The statement must be based on an examination of the relevant patent- and trademark registers. The examination takes approximately one week and costs DM 3,000.

A German company may register as many domain names as it wants. Registration of a domain name usually takes two weeks. Costs are DM 250.

England «.co.uk»

No local company requirement:
Any commercial entity, not only British, may register a domain name under «.co.uk».

Domain name registration:
Costs are GBP 80 in registration fee. A company may register as many domain names as it desires.

The Netherlands «.nl»

Local company requirement:
In the Netherlands, one must incorporate a limited liability company. The share capital requirement is Euro 18,500. In addition, there are costs in connection with a so-called «trust company», provided that the company does not want to be present or localised in the Netherlands.

In addition, there are potential costs regarding trademark registration.

Domain name registration:
Domain name registration costs NLG 100 and a yearly fee of NLG 150.

---

340. See http://www.denic.de/index.html
341. See http://www.nic.uk/
342. See http://www.domain-registry.nl/
France «.fr»

Local company requirement:
In France, one must establish a limited liability company (SARL). The share capital requirement is FRF 50,000. In addition, there are costs in connection with the incorporation, approximately FRF 20,000.

In addition, there are potential costs regarding trademark registration.

Domain name registration:
Domain name registration costs FRF 1,000, and a yearly fee of FRF 300.

Spain «.es»

Local company requirement:
In Spain, one must establish a limited liability company. The capital requirement is ESP 10,000,000. A minimum of 25% of the share capital must be paid at the incorporation.

In addition, there are potential costs regarding trademark registration.

Domain name registration:
There is only one domain name per organisation. The domain name must correspond with the company name.

Italy «.it»

No local company requirement:
In Italy, domain names are allocated on a first come, first served basis, without any prior control as to the legitimacy of such application. Any EU or Italian company or association may register an unlimited number of domain names under «.it». The domain name need not have any connection to the company name. An EU citizen may register one domain name only.

Domain name registration:
Domain name registration costs Euro 140 each for the first three domain names registered simultaneously. Then there is an additional Euro 90 for each domain name subsequent to the third. The maintenance fee applying from the second year of the life of the «.it» domain name amounts to Euro 90.

343. See http://www.nic.fr/
344. See http://www.nic.es/
345. See http://www.nic.it/
Belgium «.be» 346

No local company requirement:
In Belgium, there is a new domain name registration policy.347 The policy entered into force 11.12.00. The main changes are:

- the link between the name of the company and the domain name is abandoned
- individuals have the opportunity to register a domain name
- domain names are registered on a first come, first served basis
- domain names will be registered through a network of agents (registrars)
- the introduction of an alternative dispute resolution procedure

Domain name registration:
One may to apply for any name which is not yet registered, including generic names, and it is possible to register several domain names. However it is not possible to reserve domain names. Registration costs BEF 2.500 and a yearly fee of BEF 2.000.

Switzerland «.ch» 348

No local company requirement:
In Switzerland, the minimum share capital in a limited liability company is CHF 100.000. However, any commercial entity, not only Swiss, may register a domain name.

Domain name registration:
The registration fee is CHF 80. In addition, there is a CHF 48 yearly fee.

Austria «.at» 349

No local company requirement:
In Austria, any legal or physical person may register a domain name.

Domain name registration:
One may register directly via Internet, or by fax to Internic GmbH. Registration costs are ATS 1.500 and a monthly fee of ATS 200.

348. See http://www.nic.ch/
349. See http://www.nic.at/german/default.htm
Portugal «.pt»\textsuperscript{350}

Local company requirement:
In Portugal, one must establish a limited liability company. Minimum share capital is PTE 400,000.

Domain name registration:
Domain name registration costs PTE 14,000, plus a maintenance fee of PTE 12,000 every second year.

Ireland «.ie»\textsuperscript{351}

Local company requirement:
In Ireland, one must establish a limited liability company.

Domain name registration:
All applicants must «demonstrate a real and substantive connection with Ireland». This means that the applicant must be «a body corporate incorporated under the laws of Ireland» or «a body corporate incorporated outside Ireland and which has either established a place of business within Ireland, or has established a branch in Ireland». It is also possible to as a «a sole trader and who is registered for VAT in Ireland».

The domain name must correspond with the company name. There is no registration fee. However, there is a yearly fee of IEP 100.

Greece «.gr»\textsuperscript{352}

Local company requirement:
In Greece, a limited liability company must have a minimum share capital of GRD 10,000,000.

Domain name registration:
Any commercial entity may register up to 10 domain names. There is a requirement that the entity has «sufficient economic activity» in Greece. All trademarks registered in Greece may be registered as domain names. This applies even though the trademark owner does not have a Greek VAT number. Furthermore, an international trademark may be registered as a domain name in Greece.

\textsuperscript{350} See http://www.dns.pt/
\textsuperscript{351} See http://www.domainregistry.ie/
\textsuperscript{352} See http://www.hostmaster.gr/
Registration fee and yearly fee for the first two years GRD 15.000 in total + 18 % VAT. Two years after the registration a yearly fee of GRD 7.500 + 18 % VAT applies.

**Luxembourg «.lu»**

Any legal entity may register a domain name under «.lu», no matter where the entity is located. The domain name policy states that it is recommended that the entity is localised in Luxembourg. However, any legal entity may obtain a domain name without being situated or represented in Luxembourg. The number of domain names is unrestricted. Registration costs LUF 2000, and a yearly fee of LUF 3000.

**Croatia «.hr»**

One must establish a limited liability company in Croatia in order to obtain a domain name under «.hr». It is free to register the domain name. There is only one domain name per organisation. The name must correspond with the company name.

**Yugoslavia «.yu»**

One must establish a limited liability company or organisation registered in Yugoslavia in order to obtain a domain name under «.yu». There is only one domain name per organisation.

**Estonia «.ee»**

*Local company requirement:*  
In Estonia, one must establish a limited liability company. It is possible to buy a shelf company for approximately EEK 12.000. Minimum share capital is EEK 40.000. If the company is dormant, a «trust company» can receive mail (yearly fee EEK 3000) and act as a board member (yearly fee EEK 10.400) on behalf of the company.  
In addition comes translation costs, and costs in connection with change of company name and by-laws.

*Domain name registration:*  
The domain name must correspond with the company name.

353. See http://www.dns.lu/  
354. See http://noc.srce.hr/  
355. See http://www.nic.yu/  
356. See http://www.eenet.ee/services/subdomains.html
Hungary «.hu»\textsuperscript{357}
One must establish a limited liability company in Hungary in order to obtain a domain name under «.hu». The company may be dormant. One needs a local representative that speaks Hungarian and has an address in Hungary. Another option is to register a trademark in Hungary and then register the trademark as a domain name under «.tm.hu».

Slovakia «.sk»\textsuperscript{358}
Any commercial entity may register a domain name. A foreign applicant must register via a local representative. One may register five domain names per applicant.

Slovenia «.si»\textsuperscript{359}
A limited liability company is required in Slovenia in order to obtain a domain name under «.si». There is one domain name per organisation. The domain name must correspond with the company name.

Latvia «.lv»\textsuperscript{360}
Any legal or physical person may register a domain name. One may register directly via Internet. The applicant must send an application via Internet, and a copy of the application via post. It costs $ 100 in registration fee and $ 50 in yearly fee.\textsuperscript{361}

Litauen «.lt»\textsuperscript{362}
Any legal or physical person may register a domain name. One may register directly via Internet (hostmaster@litnet.lt). It costs Lt 200 in registration fee and Lt 80 in yearly fee. One organisation is entitled to one domain name. It is possible to argue for more domain names.\textsuperscript{363}

\textsuperscript{357} See http://www.nic.hu/
\textsuperscript{358} See http://www.sk-nic.sk/
\textsuperscript{359} See http://www.arnes.si/registracija.htm
\textsuperscript{360} See http://www.nic.lv/DNS/
\textsuperscript{361} See www.nic.lv/DNS/template.html.
\textsuperscript{362} See http://www.domreg.lt/
\textsuperscript{363} See www.domreg.lt/forma/dns_reg_en.html
Poland «.pl»

Any legal or physical person may register a domain name. One may register directly via Internet. The applicant must send an application via Internet, and a copy of the application via post. It costs 976 Pln in registration fee and 366 Pln in yearly fee. It takes approximately seven days to register a domain name.365

».com»
No company requirement. Unrestricted number of domain names.

».org»
No company requirement. Unrestricted number of domain names.

».net»
No company requirement. Unrestricted number of domain names.

6. Alternative approaches

When registering domain names under ccTLDs, one should pick the countries in which one’s products or services are offered or are likely to be offered. In those jurisdictions where registration of a branch is possible, one should try to register a branch or division. This is generally cheaper and more efficient than establishing a limited liability company.

If the domain name is identical to the company name, it is usually sufficient to establish a division. If one wants a domain name different from its company name, a limited liability company is usually necessary.

It is recommendable to also register the desired domain name as a trademark.

It is possible to make use of patent offices and Internet service providers when registering domain names. Patent offices have contact persons in several countries throughout Europe. Such offices operate with lower fees than law firms. However, a law firm may come in handy when co-ordinating simultaneous domain name registrations (and incorporating associated companies) in several countries. There is need for a co-ordinator for collection of signatures, reminders and following up the various domain name registrations. The choice thus depends on the need for fast and efficient registrations of a lot of domain names.

364. See http://www.nask.pl/
# Appendix 2
## Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPA</td>
<td>Advanced Research Projects Agency</td>
</tr>
<tr>
<td>ARPANET</td>
<td>Advanced Research Projects Agency Network</td>
</tr>
<tr>
<td>ccTLD</td>
<td>Country Code Top Level Domain</td>
</tr>
<tr>
<td>CORE</td>
<td>Council of Registrars under the gTLD-MoU</td>
</tr>
<tr>
<td>CORE MoU</td>
<td>Council of Registrars Memorandum of Understanding</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defence Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>gTLDs</td>
<td>Generic Top Level Domains</td>
</tr>
<tr>
<td>gTLD-MoU</td>
<td>Generic Top Level Domain Memorandum of Understanding</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>IESG</td>
<td>Internet Engineering Steering Group</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISOC</td>
<td>Internet Society</td>
</tr>
<tr>
<td>NOIE</td>
<td>National Office for the Information Economy</td>
</tr>
<tr>
<td>NSF</td>
<td>National Science Foundation</td>
</tr>
<tr>
<td>NSI</td>
<td>Network Solutions Inc</td>
</tr>
<tr>
<td>SLD</td>
<td>Second level Domain</td>
</tr>
<tr>
<td>SRS</td>
<td>Shared Registry System</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TLD</td>
<td>Top Level Domain</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organisation</td>
</tr>
</tbody>
</table>
TIDLIGERE UTGITT I COMPLEX-SERIEN

CompLex er Institutt for rettsinformatikks skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra GnistAkademika (se bestillingsskjema bak i boken), eller lånes på biblioteket. CompLex-serien ligger i BIBSYS.

2001

1/01 The International Sale of Digitised Products Through the Internet in a European Context
Peter Lenda...........................................................................NOK 274.50

2000

1/00 Klassikervernet i norsk åndsrett
Anne Beth Lange ...........................................................NOK 268.-

2/00 Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor
Claude A. Lenth.................................................................NOK 248.-

3/00 Innsyn i personopplysninger i elektroniske markedsplasser.
Line Coll..............................................................................NOK 148.-

1999

1/99 International regulation and protection of Internet domain and trademarks
Tonje Røste Gulliksen......................................................NOK 248.-

2/99 Betaling via Internett
Camilla Julie Wollan............................................................NOK 268.-
3/99 Internett og jurisdiksjon
Andreas Frølich Fuglesang & Georg Philip Krog ...........NOK 198.-

1998

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

2/98 Straffbar hacking, straffelovens § 145 annet ledd
Guru Wanda Wanvik .....................................................NOK 238.-

3/98 Interconnection - the obligation to interconnect telecommunications networks under EC law
Katinka Mahieu .............................................................NOK 198.-

1997

1/97 Eksempelarfremsattelse av litterære verk til privat bruk
Therese Steen .................................................................NOK 158.-

2/97 Offentlige anskaffelser av informasjonsteknologi
Camilla Sivesind Tokvam ................................................NOK 175.-

3/97 Rettslige spørsmål knyttet til Oppgaveregisteret
Eiliv Berge Madsen .......................................................NOK 170.-

4/97 Private pengespill på Internett
Halvor Manshaus ...........................................................NOK 160.-

5/97 Normative Structures in Natural and Artificial Systems
Christen Krogh ...............................................................NOK 255.-

6/97 Rettslige aspekter ved digital kringkasting
Jon Bing .........................................................................NOK 178.-

7/97 Elektronisk informasjonsansvar
Tomas Myrbostad ...........................................................NOK148.-
8/97  Avtalelisens etter åndsverksloven § 36
Ingrid Mauritzen............................................................NOK 120.-

9/97  Krav til systemer for forvaltning av immaterielle rettigheter
Svein Engebretsen ..........................................................NOK 168.-

10/97 American Telephony: 120 Years on the Road to Full-blown Competition
Jason A. Hoida ..............................................................NOK 140.-

11/97 Rettslig vern av databaser
Harald Chr Bjelke..........................................................NOK 358.-

1996

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

2/96 Public Policy and Legal regulation of the Information Market in the Digital Network Enviroment
Stephen John Saxby .......................................................NOK 238.-

3/96 Opplysning på spill
Ellen Lange....................................................................NOK 218.-

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

5/96 Fjernarbeid
Henning Jakhelln ...........................................................NOK 235.-

6/96 A Legal Advisory System Concerning Electronic Data Interchange within the European Community
Andreas Mitrakas...........................................................NOK 128.-

7/96 Elektronisk publisering: Utvalgte rettslige aspekter
Jon Bing og Ole E. Tokvam ...........................................NOK 186.-

8/96 Fjernsynsovervåking og personvern
Finn-Øyvind H. Langfjell..............................................NOK 138.-
1995

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

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

3/95  Legal Expert Systems: Discussion of Theoretical Assumptions  
Tina Smith ...............................................................................................................NOK 278.-

4/95  Personvern og straffeansvar - straffelovens § 390  
Ole Tokvam ..........................................................................................................NOK 198.-

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

6/95  Public Administration and Information Technology  
Jon Bing and Dag Wiese Schartum .................................................................NOK 348.-

7/95  Law and Liberty in the Computer Age  
Vittorio Frosini ....................................................................................................NOK 158.-

1994

1/94  Deon'94, Second International Workshop on Deontic Logic in Computer Science  
Andrew J. I. Jones & Mark Sergot (ed) ......................................................NOK 358.-

2/94  Film og videogramrett. TERESA (60)  
Beate Jacobsen .....................................................................................................NOK 318.-
3/94 Elektronisk datutveksling i tollforvaltningen - Rettslige spørsmål knyttet til TVINN  
Rolf Risnæs .................................................................................NOK 225.-

4/94 Sykepenger og personvern - Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd  
Mari Bø Haugestad .....................................................................NOK 148.-

5/94 EØS, medier og offentlighet. TERESA (103)  
Mads Andenæs, Rolf Høyer og Nils Risvand ..............................NOK 148.-

6/94 Offentlige informasjonstjenester: Rettslige aspekter  
Jon Bing ......................................................................................NOK 148.-

7/94 Sattelittfjernsyn og norsk rett. MERETE (3) IV  
Nils Eivind Risvand .....................................................................NOK 138.-

8/94 Videogram på forespørsel. MERETE (14) IV  
Beate Jacobsen (red) ....................................................................NOK 158.-

9/94 «Reverse engineering» av datamaskinprogrammer. TERESA (92) IV  
Bjørn Bjerke ...............................................................................NOK 198.-

10/94 Skattemessig behandling av utgifter til anskaffelse av datamaskinprogrammer. TERESA (75)  
Gjert Melsom ..............................................................................NOK 198.-

1993

1/93 Artificial Intelligence and Law. Legal Philosophy and Legal Theory  
Giovanni Sartor ..........................................................................NOK 148.-

2/93 Erstatningsansvar for informationstjenester, særlig ved databaseydelser  
Connie Smidt .............................................................................NOK 138.-

3/93 Personvern i digitale telenett  
Ingild Hanssen-Bauer ....................................................................NOK 178.-
4/93 Consumers Purchases through Telecommunications in Europe. - Application of private international law to cross-border contractual disputes
   Joachim Benno ...............................................................NOK 198.-

5/93 Four essays on: Computers and Information Technology Law
   Morten S. Hagedal .........................................................NOK 218.-

6/93 Sendetidsfordeling i nærradio MERETE (3) III
   Marianne Rytter Evensen ...............................................NOK 148.-

7/93 Essays on Law and Artificial Intelligence
   Richard Susskind ............................................................NOK 158.-

1992

1/92 Avskriving av mikrodatamaskiner med tilbehør – en nordisk studie
   TERESA (87)
   Beate Hesseltvedt ...........................................................NOK 138.-

2/92 Kringkastingsbegrepet TERESA (78)
   Nils Kr. Einstabland .......................................................NOK 208.-

3/92 Rettskilderegistre i Helsedirektoratet NORIS (94) I & II
   Maria Strøm .....................................................................NOK 228.-

4/92 Softwarepatent – Imaterialretts enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindelser i amerikansk og europæisk ret
   Ditlev Schwanenfügel ....................................................NOK 158.-

5/92 Abonnementskontrakter fra kabelfjernsyn TERESA (78II)
   Lars Borchgrevink Grindal ............................................NOK 248.-

6/92 Implementing EDI - a proposal for regulatory form
   Rolf Riisnæs .................................................................NOK 118.-

7/92 Deponering av kildekode «escrow»-klausuler TERESA (79)
   Morten S. Hagedal ..........................................................NOK 128.-
8/92  EDB i juridisk undervisning – med en reiserapport fra England og USA
     Ola-Kristian Hoff ..............................................NOK 228.-

9/92  Universiteters ansvar for bruk av datanett TERESA (94)
     Jon Bing & Dag Elgesem .....................................NOK 198.-

10/92 Rettslige sider ved teletorg
      Andreas Galtung .............................................NOK 148.-
BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Nummer / årgang:  
Tittel:  

Nummer / årgang:  
Tittel:  

Nummer / årgang:  
Tittel:  

Nummer / årgang:  
Tittel:  

Navn:  
Adresse:  
Postadresse:  
Telefon:  

Bestillingsskjemaet sendes pr.post eller telefaks til:

Avd. juridisk litteratur Aulabygningen  
Karl Johansgt. 47, 0162 Oslo  
Telefon: 22 42 54 50  
Telefaks: 22 41 17 08  
CompLex kan også bestilles via nettbokhandelen www.gnist.no