

GRADUATE THESIS, 20P
FACULTY OF LAW, UNIVERSITY OF LUND,
SWEDEN
SUPERVISOR: PROFESSOR LENNART
SVENSÄTER

INTELLECTUAL
PROPERTY ISSUES IN
CYBERSPACE

© Johan Carl Sjöbeck 1998

Preface

I would like to take this opportunity to thank my dear parents, Bo and Barbro. Without their warm support in numerous ways, it would definitely have been more burdensome to write this thesis. By supplying me with computers since my early teens, they undoubtedly awakened my interest for computers. I owe my parents everything. I would also like to thank Cristina Landgren for patiently listening to my tedious monologues regarding the issues in this thesis and for giving valuable advice. I am also very grateful to Professor Lennart Svensäter, who believed in this subject and agreed to let me write the thesis under his supervision.

Content

1	INTRODUCTION.....	1
2	BRIEF HISTORY OF THE EVOLUTION AND GROWTH OF THE INTERNET	3
3	HYPERLINKING.....	4
3.1	HYPertext LINKS.....	4
3.2	INLINE LINKING	6
3.3	FRAMING.....	6
3.4	THE WASHINGTON POST COMPANY ET AL V. TOTAL NEWS, INC.	7
3.4.1	<i>The framed sites were displayed in a distorted way</i>	7
3.4.2	<i>Potential confusion among users regarding the origin of the news.....</i>	8
3.4.3	<i>“Voluntary” settlement.....</i>	8
3.5	TICKETMASTER V. MICROSOFT	9
3.5.1	<i>Microsoft’s site linked to the extremely popular Ticketmaster site.....</i>	9
3.5.2	<i>The lawfulness of hypertext links</i>	9
3.6	SHETLAND NEWS	10
3.6.1	<i>The interim injunction is not the death of hyperlinking in the U.K.....</i>	10
3.6.2	<i>Newspaper headlines on a website may enjoy copyright.....</i>	11
3.6.3	<i>URL may enjoy copyright.....</i>	11
3.6.4	<i>Fair dealing and implied license when copying URLs and news headlines</i>	11
3.6.5	<i>Settlement reached in November 1997</i>	12
3.7	HYPertextS IN A SWEDISH PERSPECTIVE: MAKING A LINK IS NOT EQUIVALENT OF PRODUCING A COPY OF THE MATERIAL LINKED TO	12
4	CACHING	14
4.1	CACHING IS SOMETIMES CONSIDERED A COPYRIGHT INFRINGEMENT	14
4.2	LEGAL CONSIDERATIONS CONCERNING BROWSING.....	15
4.3	THE INCREASING USAGE OF PASSWORDS AND USER IDS SUPPORTS THE EXISTENCE OF AN IMPLIED LICENSE TO VISIT PUBLIC-ACCESS SITES	15
4.4	MAI SYSTEMS CORPORATION V. PEAK COMPUTER INC.....	16
4.4.1	<i>A copy stored in the RAM is considered a fixed copy under the Copyright Act</i>	16
4.4.2	<i>The rightful possessor of a computer program cannot authorize a third party to make a copy</i>	17
4.5	TRIAD SYSTEMS CORP. V. SOUTHEASTERN	17
4.5	EXPRESS CO.....	18
4.5.1	<i>Defense of fair use rejected</i>	18
4.6	SUMMARY	19
5	PROXYCACHING	20
5.1	THE LEGAL DILEMMA OF PROXYCACHING	20
5.1.1	<i>Page impressions.....</i>	20
5.1.2	<i>A proxycached site constitutes a copy</i>	21
5.1.3	<i>Fair use to utilize proxycaching</i>	21
5.2	PROXYCACHING IN A SWEDISH LEGAL PERSPECTIVE	21
5.3	SUMMARY	22
6	DOMAIN NAMES.....	23
6.1	INTERNET PROTOCOL ADDRESSES	23
6.2	TOP LEVEL DESIGNATORS.....	23
6.3	SECONDARY LEVEL DESIGNATORS	24
6.4	THE NEED FOR A UNIVERSAL DOMAIN DIRECTORY SERVICE	24

6.5	REGISTERING DOMAIN NAMES IN THE UNITED STATES	25
6.5.1	<i>The domain name dispute policy</i>	25
6.6	REGISTERING DOMAIN NAMES IN SWEDEN.....	26
6.7	CYBERSQUATTING.....	27
6.7.1	<i>Reasons why one ought to fight a cybersquatter</i>	27
6.7.2	<i>Hostile takeover of trademark by cybersquatter</i>	28
6.8	CONFUSING DOMAIN NAMES.....	28
6.9	POSSIBLE CONFLICTS BETWEEN DOMAIN NAMES AND TRADEMARKS	28
6.10	TRADEMARKS AND DOMAIN NAMES IN SWEDEN.....	29
6.11	DOMAIN NAMES ARE NOT SOLELY DESCRIPTIVE	30
6.12	REGISTERING A TRADEMARK CONSISTING OF A gTLD	30
6.13	THE POSSIBILITIES OF DOMAIN NAMES INFRINGING UPON ALREADY EXISTING TRADEMARKS AND VICE VERSA	31
6.14	DOMAIN NAME INFRINGEMENTS AND DISPUTES	31
6.15	MTV NETWORKS V. ADAM CURRY	32
6.16	ROADRUNNER V. NSI.....	32
6.16.1	<i>Hostile takeovers of domain names</i>	33
6.17	SUMMARY	34
7	INTELLECTUAL PROPERTY PIRACY IN CYBERSPACE.....	35
7.1	RESPONSIBILITY FOR POSTING, STORING AND DOWNLOADING PROTECTED MATERIAL 35	
7.2	THE FIRST COPY MADE FROM THE ORIGINAL SOURCE OUTSIDE CYBERSPACE	36
7.2.1	<i>Copying software off-line</i>	36
7.2.2	<i>Copying music off-line</i>	37
7.2.3	<i>Copying pictures off-line</i>	38
7.3	LEGAL RESPONSIBILITY WHEN POSTING PROTECTED MATERIAL IN CYBERSPACE....	38
7.3.1	<i>Uploading software</i>	38
7.3.1.1	Uploading is not equivalent of private copying.....	38
7.3.1.2	On-line backup copy	39
7.3.1.3	The uploading person is responsible	39
7.3.2	<i>Uploading pictures</i>	39
7.3.3	<i>Uploading music</i>	40
7.3.3.1	Uploading MP3 files to a website.....	41
7.3.3.2	Background music on websites	41
7.4	THE LEGAL RESPONSIBILITIES OF ISPs AND BBS OPERATORS	42
7.4.1	<i>The monitoring of posted information</i>	42
7.4.1.1	The most suitable supervisor	43
7.4.1.2	Transferring the responsibility from the ISP to the subscriber	44
7.4.2	<i>Cyberspace without ISP liability</i>	45
7.4.2.1	The U.S. ISP exemption	45
7.4.3	<i>European proposals concerning ISP liability</i>	46
7.4.4	<i>Cases suggesting that ISPs or BBS operators have a legal responsibility</i> ..	46
7.4.4.1	NJA 1996:74	46
7.4.4.2	Playboy Enterprises v. Frena	47
7.4.4.3	Sega Enterprises Ltd. V. Maphia.....	47
7.4.5	<i>Cases denying ISP or BBS operator responsibility</i>	48
7.4.5.1	NJA 1996:79 “The BBS-case”	48
7.4.5.2	Zeran v. America Online	49
7.4.5.3	Doe v. America Online Inc.....	50
7.4.6	<i>Music archives in Cyberspace</i>	50
7.5	LEGAL RESPONSIBILITY WHEN DOWNLOADING PROTECTED MATERIAL	51
7.5.1	<i>Responsibility when downloading software from the Internet</i>	52
7.5.2	<i>Responsibility when downloading music from the Internet</i>	53
7.6	SUMMARY	54
8	JURISDICTION.....	56
8.1	THE IMPORTANCE OF JURISDICTION IN THE WORLD OF INFORMATION TECHNOLOGY 56	

8.2	SWEDISH RULES CONCERNING JURISDICTION	57
8.3	U.S. JURISDICTION ISSUES IN BRIEF	58
9	AMERICAN CASES IN WHICH JURISDICTION IS GRANTED	60
9.1	UNITED STATES V. THOMAS.....	60
9.1.1	<i>The California website distributed obscene material in Tennessee.....</i>	60
9.1.2	<i>The obscene downloaded material did leave the Californian website.....</i>	60
9.1.3	<i>Refusing customers in certain jurisdictions in order to diminish risk of liability</i>	61
9.2	INSET SYSTEMS, INC. V. INSTRUCTIONS SET, INC.	61
9.2.1	<i>Website advertisement fulfilled the “minimum contacts test”</i>	61
9.3	PLAYBOY ENTERPRISES V. CHUCKLEBERRY PUBLISHING INC.....	62
9.3.1	<i>Placing information on an Italian server is equivalent</i>	62
9.3.1	<i>of distributing the information within the U.S.</i>	63
9.3.2	<i>Italian publisher ordered to ignore U.S. users or shut down the site.....</i>	63
9.4	COMPU SERVE V. PATTERSON	63
9.4.1	<i>A few sales via the Internet are considered sufficient contacts.....</i>	64
9.4.2	<i>Stubborn focus on the physical placement of the server.....</i>	64
9.4.3	<i>Possibility of “server havens” in remote locations</i>	65
9.5	MARITZ, INC. V. CYBERGOLD, INC.....	65
9.5.1	<i>Minimum contacts.....</i>	66
9.5.2	<i>The intent of setting up a site can decide whether it is classified as passive or active</i>	66
9.6	PANAVISION INTERNATIONAL, L.P, V. DENNIS TOEPPEN	67
9.6.1	<i>The three-part test concerning specific jurisdiction</i>	67
9.7	STATE OF MINNESOTA V. GRANITE GATE RESORTS INC.....	68
9.7.1	<i>Las Vegas Internet advertisement violated Minnesota consumer protection</i>	68
9.7.2	<i>A disclaimer on the website not enough to avoid Minnesota jurisdiction ...</i>	69
9.7.3	<i>Internet advertisements more pervasive than traditional advertisements....</i>	69
9.8	HEROES, INC. V. HEROES FOUNDATION	70
9.8.1	<i>A website and advertisement in a newspaper is enough to exercise jurisdiction in Columbia</i>	71
9.9	ZIPPO MANUFACTURING CO. V. ZIPPO DOT COM, INC.	71
9.9.1	<i>The level of commercial activity and interactivity of websites.....</i>	72
9.9.2	<i>Entering into contract and transmitting computer files via the Internet.....</i>	72
9.9.3	<i>Passive websites.....</i>	72
9.9.4	<i>Interactivity.....</i>	73
9.9.5	<i>The Dot Com website was more than interactive.....</i>	73
9.9.6	<i>Analogy between passive websites and paperback advertisements</i>	73
9.10	CODY V. WARD.....	74
9.10.1	<i>Fifteen e-mails and a four phone calls fulfills the requirement of purposeful minimum contacts with Connecticut</i>	74
9.11	DIGITAL EQUIPMENT CORP. V. ALTAVISTA TECHNOLOGY INC.	75
9.11.1	<i>Confusingly similar websites</i>	75
9.11.2	<i>A constantly accessible website is a sign of conducting business in Massachusetts</i>	76
9.11.3	<i>Consequences of business in Cyberspace should be considered in advance</i>	76
9.11.4	<i>Cost efficiency and jurisdiction</i>	76
9.12	HALL V. LARONDE.....	76
9.12.1	<i>E-mail and telephone calls were the only contacts between the parties</i>	77
9.12.2	<i>General personal jurisdiction.....</i>	77
9.12.3	<i>Specific personal jurisdiction</i>	77
9.12.4	<i>Minimum contacts can be electronic</i>	77
9.12.4.1	<i>People v. Lipsitz.....</i>	78
9.12.5	<i>No alternative treating of Cyberspace issues</i>	78
9.12.6	<i>Jurisdictional considerations.....</i>	79

10	AMERICAN CASES IN WHICH JURISDICTION IS REFUSED.....	80
10.1	PRES-KAP INC. V. SYSTEM ONE, DIRECT ACCESS INC.	80
10.1.1	<i>Placement of server irrelevant.....</i>	80
10.2	BENSUSAN RESTAURANT CORP. V. RICHARD B. KING.....	81
10.2.1	<i>A general, passive website does not focus on any particular jurisdiction... </i>	81
10.2.2	<i>Three factors determining jurisdiction</i>	82
10.2.3	<i>A general, passive website alone cannot subject a web-editor to other forum's jurisdictions</i>	82
10.3	HEARST CORPORATION. V. ARI GOLDBERGER	83
10.3.1	<i>A website is analogous to a traditional advertisement in a paper magazine</i> <i>83</i>	
10.3.2	<i>Jurisdiction based upon solely a website would create</i>	83
10.3.2	<i>worldwide jurisdiction.....</i>	84
10.3.3	<i>A website directed at the whole world could be equivalent of a national magazine.....</i>	84
10.4	CYBERSELL, INC., V. CYBERSELL, INC.....	84
10.4.1	<i>Three-part test in order to exercise specific jurisdiction.....</i>	85
10.4.2	<i>Solely a website did not trigger jurisdiction.....</i>	85
10.4.3	<i>A passive site with no commercial activities relating to the jurisdiction.....</i>	86
10.4.4	<i>Mc.Donough v. Fallon McElligott, Inc.....</i>	86
11	CONCLUSION REGARDING THE CASES INVOLVING JURISDICTION..	87
11.1	INTERACTIVITY AND PASSIVITY	87
11.2	DISCLAIMERS	88
11.3	AVAILING ONESELF OF THE PRIVILEGE OF CONDUCTING BUSINESS WITHIN THE FOREIGN JURISDICTION.....	88
11.4	THE PHYSICAL LOCATION OF SERVERS AND DATABASES.....	88
11.5	E-MAIL CONTACTS.....	89
12	THE ROLE OF NATIONAL LEGAL FRAMEWORKS IN A MULTINATIONAL CYBERWORLD.....	90
12.1	VIRTUAL CYBERCOURTS	90
12.2	INTERNATIONAL COPYRIGHT TREATIES.....	90
13	CONCLUSION.....	92

1 Introduction

In the modern society of today, it is difficult not to be influenced in any way by the rapidly evolving computer technology that enables people to communicate without respect to geographical or national borders at a remarkable low cost. One could say that Cyberspace is growing with such confidence and speed, that it may very well become an additional world, parallel to the “real” world. Authorities, companies and individuals around the globe are on the edge of realizing the vast potentials of this new swelling electronic world. If one chooses to enter Cyberspace, one can be seen everywhere, be contacted by anyone and contact anyone, no matter where the parties are physically situated on the globe. I am of the opinion that it is fair to say that this new world is saturated with digitized information of varied quality and importance. Due to the fact that all information is digitized, virtually everyone can reproduce everything flowing through the giant system. Intellectual property, as a whole, has never experienced such a hazardous environment, as it does in Cyberspace. In this thesis I will try to point out the new rapidly developing dangers concerning intellectual property in Cyberspace. Since one cannot investigate and analyze everything about everything, one is unfortunately forced to limit the thesis to cover merely a few areas of this extremely interesting field. I have chosen to study various intellectual property issues from a Swedish perspective. However, since the Swedish legal system at this point in time only is on the verge of grasping the potential dangers to intellectual property in Cyberspace, I have chosen to investigate and focus intensively on the legal developments concerning these issues in the U.S. Since Europe is roughly lagging two or three years behind the U.S. regarding the Internet, I believe it is of highest importance to study their problems and possibly be able to take advantage of some of their legal solutions. Even though the legal systems are completely different, one should not completely ignore the American case law, because such cases may provide helpful guidance to various problems that may arise in Cyberspace. One must realize that Cyberspace is not at all bound by any national borders. It is a universal region where all the legal systems of the world may intersect in one way or another.

The material I have studied consists of laws, legal literature, legal articles, cases and various other legal documents. Many of the sources I have utilized are electronic, and I have supplied all the web addresses in the footnotes, in order to facilitate further reading. The dates supplied after the websites indicate the day the sites were viewed. Primarily, I briefly describe the history of the Internet before describing specific Internet related problems, such as linking, caching, proxycaching and domain names. After this, I describe the various problems of intellectual property piracy, and determine who is responsible when music, software and pictures are copied, uploaded, stored and downloaded. I describe the problems concerning ISP and BBS-operator liability. In addition to this, I have chosen to study the problem of

jurisdiction in Cyberspace. If one does not know which jurisdiction that is considered the proper one, there is a risk that much of one's national legal knowledge concerning intellectual property becomes superfluous. It is important to know where one can sue and which country's laws that are applicable and which ones that are not.

2 Brief history of the evolution and growth of the Internet

It is not until recently that the Internet has become an important everyday tool for all various sorts of people around the globe. The origins of the Internet are normally traced back to the Advanced Research Projects Agency's developments undertaken by the American Department of Defense in the 1960s. Some of the basic concepts from these days have been refined and modified and are no longer solely serving military purposes, such as e-mail, file transfers etc. In those days, not much but unformatted text-transfers were supported. One crucial factor of the enormous success of the Internet lies in the fact that it encourages transmission not only of text, but also of various kinds of complicated graphics. In the future, the amount of users having an Internet access with sufficient bandwidth¹ may play an important role since the applications are rapidly becoming larger and tend to use up more and more bandwidth.² Today, the very heavy traffic of packets flowing through the wires containing real-time graphic and audio etc has lead to a severe congestion of the telecommunication infrastructure. Once the problem of congestion is solved, a great deal more audiovisual packets may be able to pass through the cables. Internet connection through satellites is the latest development in the area. The accelerating developments in these fields have and will lead to numerous new problems concerning intellectual property around the globe. We are only in the beginning of a new era of intellectual property.

¹ Bandwidth is a measure of data transmission capacity of a system or channel.

² *The Future of the Internet – What Role for Europe?* Interim Report of an Advisory Group 970311. [Http://www.cordis.lu/esprit/src/i2eurepo.htm](http://www.cordis.lu/esprit/src/i2eurepo.htm) (970805)

3 Hyperlinking

In order to provide more interesting websites, to make surfing easier, more efficient and less time consuming, most websites today provide various kinds of hyperlinks. Hyperlinking has proven to be an essential part of the success of the Internet as a resource and financially profitable medium.³ The ability to link to other sources of information surely has revolutionized information retrieval as well as reading documents. Hyperlinks are points in web documents through which users may transport themselves directly to another website or retrieve information without typing a new location in the Uniform Resource Locator (URL). The traditional method of finding and retrieving documents requires the browser to know the exact address required in the URL and type it by hand or equivalent. Once the complete and exact address is typed in the URL, the search for the address begins, and the user is transported to the new desired location. The utilization of hyperlinks makes knowledge of the exact addresses as well as the manual typing obsolete. If the active web document displays a link to another site, file or place within the same document, and the user clicks on it with the mouse, he/she will instantly, without typing, be transported in one way or another to the linked page, file or place. The three most important methods of linking are hypertext links, inline links and framing.

3.1 Hypertext links⁴

Hyperlinking is one of the strengths of the World Wide Web, allowing users to jump from one Internet site to another. Hypertext links (Hypertext Reference links are often called HREF links) is the most widely used linking method in Cyberspace. Hypertext links are very convenient, since the hyperlinks are imbedded in a piece of text without hindering the reader nor using too much memory as pictures sometimes have a tendency to do. Often the link is differentiated from the rest of the text material by the way it is displayed. It can for example consist of a highlighted or underlined word, indicating to the surfer that it is a "footnote-like" link to another Internet location. Once the surfer activates the hypertext link by clicking on it, the computer immediately establishes a new connection with a site on another server (inter-system linking)⁵ that is linked to (linking out)⁶. Alternatively there can be a link to another place in the same document (intra-page

³ *Frame Liability Clouds the Internet's Future*, The New York Law Journal, May 19, 1997. [Http://www.ljx.com/Internet/0519nyframe.html](http://www.ljx.com/Internet/0519nyframe.html) (971006).

⁴ This part is based on *Dangerous Liaisons: The Legal Risks of Linking Web Sites*, Richard Raysman and Peter Brown, The New York Law Journal, April 8, 1997. [Http://www.ljx.com/Internet/0408lias.html](http://www.ljx.com/Internet/0408lias.html) (971006)

⁵ *Linking Copyright to Homepages*, Matt Jackson. [Http://www.law.indiana.edu/fclj/v49/no3/jackson.html](http://www.law.indiana.edu/fclj/v49/no3/jackson.html)

⁶ *Freedom to Link Under Attack*, The New York Law Journal, June 23 1997. [Http://www.ljx.com/Internet/0623link.html](http://www.ljx.com/Internet/0623link.html) (971006)

linking)⁷ or to another document on the same server (intra-system linking)⁸. At this point in time, only one document can be viewed at a time using standard hypertext links.

The linking site can link to another site without the other author's knowledge or consent unless special security measures are taken. Some claim that permission is required when including a link to another's site. It is still not possible to link to a specific picture or word in the other site unless the graphics or word has an URL address of its own.⁹ However, if anchors are used, it is possible to link directly to subsections of a document. An anchor is an HTML tag¹⁰ that marks a specific point in an HTML document as either the source or destination of a hypertext link. This allows anyone to create links from one hypertext document to another, as well as to different sections within the same document.

Basically, there are two important and interesting legal questions concerning links. Firstly, there is the question whether linking to another site, without permission is lawful and secondly, the question whether the linker is responsible for any of the content in the site that has been linked to. It may in some instances be a question of contributory copyright infringement.¹¹ Some web authors are opposed to linking without permission, since it is in a way a matter of freeriding. For example, the Georgia Computer Systems Protection Act¹² could be interpreted as forbidding linking without consent from the linked-to site. A site without any individual content of its own can link to many other sites in order to make the site more useful and at the same time give the site an extra touch of excitement. If a site contains numerous links to various interesting pages, it could function as a frequently visited starting point for many users of the web. Often, links go straight to the most popular pages, thus bypassing all the pages preceding them. Why do some people consider this inappropriate? One must look the web of today as a grand market for advertising and advertising revenues. If sites containing advertising banners are bypassed as a result of direct links that plough deep into the sites, the number of hits decrease on the main front sites and consequently fewer advertisers choose to place their banners there. The

⁷ *Linking Copyright to Homepages*, Matt Jackson.
[Http://www.law.indiana.edu/fclj/v49/no3/jackson.html](http://www.law.indiana.edu/fclj/v49/no3/jackson.html)

⁸ *Ibid.*

⁹ *Linking Copyright to Homepages*, Matt Jackson.
[Http://www.law.indiana.edu/fclj/v49/no3/jackson.html](http://www.law.indiana.edu/fclj/v49/no3/jackson.html)

¹⁰ Anchors that point to different places in the same document use the <A NAME> tag and are used to navigate long documents with many sections. Anchors that point to other hypertext documents use the <A HREF> tag.

[Http://www.glossary.com](http://www.glossary.com) (971014).

¹¹ *Linking Rights*, Brad Templeton. [Http://www.clari.net/brad/linkright.html](http://www.clari.net/brad/linkright.html) (971021)

¹² Georgia Computer Systems Protection Act 16-9-93.1
[Http://www.mindspring.com/~ajc10/galaw.html](http://www.mindspring.com/~ajc10/galaw.html) (980215)

advertisers may choose to place their ads in the middle of the most popular (linked to) pages, such as in the middle of a news report. They may perhaps choose to advertise on the popular linking sites instead, if it will generate a greater number of hits than the sites that are linked to. The linking site created no material of its own, except for the compilation of links to other sites. This was the case in *The Washington Post Company et al v. Total News, Inc.*¹³ which will be analyzed further below.

3.2 Inline linking¹⁴

Another way of linking web documents is through *inline links* (Inlined images, known as IMG). IMGs are graphics displayed on webpages. An IMG link is automatically activated as the page is first loaded into the Random Access Memory (RAM), and is often used by the web-editors to bring graphic images into and around the text on a page. The graphics are stored in separate files and often they are part of material belonging to other websites (linking in).¹⁵ One could say that these graphic files are automatically loaded into the page, as the user is waiting for the content of the site to emerge. To a user, it may look as if the linking site is authorized to use the graphic material that was transported from the site linked to. In certain circumstances, this may lead to situations where users receive false confidence in sites. In most cases, however, the average user would not be aware that the image was incorporated into the document automatically from a remote site, and not stored locally. To most people it does not matter at all, from where the requested information comes.

3.3 Framing¹⁶

Framing is another method of linking to other remote sites. Since the introduction by Netscape Communications Corp. in January 1996 with the release of Navigator 2, it has developed to be a very popular tool frequently used in many websites around the world.¹⁷ Today, most browsers support frames. By utilizing frames it is possible to divide a page into several frames or windows that are scrollable regions operating independently of each other. The special feature of framing, compared to the other possibilities of linking, is the fact that the webpage that frames a remote site incorporates

¹³ *Washington Post Company et al. V. Total News Inc.*, U.S. District Court, Southern District of New York, 97 Civ.1190(PKL).

[Http://www.ljx.com/Internet/totalse.htm](http://www.ljx.com/Internet/totalse.htm) (971011)

¹⁴ *Dangerous Liaisons: The Legal Risks of Linking Web Sites*, Richard Raysman and Peter Brown, The New York Law Journal, April 8, 1997.

[Http://www.ljx.com/Internet/0408lias.html](http://www.ljx.com/Internet/0408lias.html) (971006)

¹⁵ *Freedom to Link Under Attack*, The New York Law Journal, June 23 1997.

[Http://www.ljx.com/Internet/0623link.html](http://www.ljx.com/Internet/0623link.html) (971006)

¹⁶ *Dangerous Liaisons: The Legal Risks of Linking Web Sites*, Richard Raysman and Peter Brown, The New York Law Journal, April 8, 1997.

[Http://www.ljx.com/Internet/0408lias.html](http://www.ljx.com/Internet/0408lias.html) (971006)

¹⁷ *'Framing': Internet Equivalent of Pirating?*, The New York Law Journal April 4 and 11, 1997 (published in two parts)

[Http://www.ljx.com/Internet/0411frame.html](http://www.ljx.com/Internet/0411frame.html)

the framed site *into* its own page. A whole site or only a part of a site can be framed. The controversy regarding this phenomenon is that the framed site is surrounded by the framers' own site or frame. As a result, the framer can transport the contents of a remote site to his own site and imbed this into his own design, surrounded by advertising belonging to him. The user may not understand that the content of the framed site originates from a remote site, since the URL of the framed site will not be displayed. The URL will still be that of the framing site and not of the framed site. This is likely to cause confusion and uncertainty concerning the origin of information displayed on screen. It may falsely give the impression that the original site is authorized to use the material of the framed site, like mentioned above at the IMG link. This was a very crucial issue in *The Washington Post Company et al v. Total News, Inc.*¹⁸

3.4 The Washington Post Company et al v. Total News, Inc.¹⁹

Total News used framing technology in order to put all the major web news sources together in one site on the Internet. This was a purely commercial site, since the Total News generated revenue by selling advertisement space on the site. Several large news providers such as The Washington Post, CNN, Los Angeles Times, Dow Jones & Company and Reuters were framed by Total News. They all sued Total News on February 20 1997, claiming that by framing their content Total News pirated copyrighted material and acted as a parasitic site, since Total News did not provide much, if any, content of its own. The news sites claimed that Total News practice of framing the content of the other websites constituted misappropriation, federal trademark infringement, dilution and false designation of origin and copyright infringement. Total News did not own any famous trademarks and created no copyrighted news stories itself. Total News solely provided the framing links in order to attract as many users as possible, and thus created a popular site in order to attract more advertisers and generate more revenues. Advertising has become an important source of revenue for many websites. According to the complaint²⁰ it is estimated that for the first three quarters of 1996, over \$150 million was spent on advertising on websites.

3.4.1 The framed sites were displayed in a distorted way

None of the framed sites appeared in the form originally intended when framed. They were altered in various ways, such as diminished size or cut in order to fit into intended portions of the Total News site. As the framed news sites were displayed in windows of the Total News site, these were

¹⁸ *Washington Post Company et al. V. Total News Inc.*, U.S. District Court, Southern District of New York, 97 Civ.1190(PKL).
[Http://www.ljx.com/Internet/totalse.htm](http://www.ljx.com/Internet/totalse.htm) (971011)

¹⁹ *Ibid.*

²⁰ Complaint: *The Washington Post Company v Total News, Inc.* at 5. (Dated Feb. 20 1997) [Http://www.ljx.com/Internet/complain.html](http://www.ljx.com/Internet/complain.html) (971006)

totally surrounded by material unrelated to the original content of the framed news sites. This created a situation where the advertisements of the framed news sites were very diminished and cut in size and had to compete with the advertisements displayed on the Total news site as well with the visual clutter of the actual “totalnews.com” frame. This is serious, since a copyright owner’s rights may be infringed if the material is altered, modified or presented to the public in a distorted form.²¹ There was a possibility that the advertisements from the framed sites and those from the Total News would be directly competitive. The advertisers of the framed news sites were not obtaining the kind of presentation they paid for. One must keep in mind, that the Total News site never altered or changed any material belonging to the other news sites. Total News merely presented the contents of these sites in its own way in its own site.

3.4.2 Potential confusion among users regarding the origin of the news

Surfers could have been confused concerning the origin of the information displayed on the Total News site, since the URL only displayed the address of Total News and not the addresses of the framed sites. It may be argued that one could receive the impression that Total News was the author of the displayed news belonging to the other sites. Surfers could also receive the impression that Total News was in some way sponsored by the well known news sites, or that the sites were associated.

3.4.3 “Voluntary” settlement

A settlement²² was reached on June 5 1997, prohibiting Total News from framing the other news sites. Total News was not allowed to display any logos etc. relating to the other news sites. However, Total News was permitted to use ordinary tedious HREF hyperlinking in the form of plain text that is highlighted. This will completely transport the user to the desired news site, instead of bringing the desired news site to the user within the Total News frame. Total News was not allowed to use alternative means of framing, such as using an indirect link via a third-party website from which users of the Total News site would be able to view the other news sites via a frame. One must keep in mind that this is only a “voluntary” settlement, and not a ruling by a court. Until such a ruling is given, this settlement may *de facto* set the standards for hyperlinking.²³

²¹ *Frame Liability Clouds the Internet’s Future*, The New York Law Journal, May 19, 1997. [Http://www.ljx.com/Internet/0519nyframe.html](http://www.ljx.com/Internet/0519nyframe.html) (971006).

²² *Washington Post Company et al. V. Total News Inc.*, U.S. District Court, Southern District of New York, 97 Civ.1190(PKL).

[Http://www.ljx.com/Internet/totalse.htm](http://www.ljx.com/Internet/totalse.htm) (971011)

²³ *Lag och rätt på Internet*, Thomas Carlén-Wendels, page 98.

3.5 Ticketmaster v. Microsoft

Ticketmaster is a company engaged in the business of providing automated ticketing services to various arenas and places throughout the United States. Ticketmaster owns a website on the Internet called "www.ticketmaster.com" and according to the complaint²⁴ filed by Ticketmaster on May 8, 1997, it is extremely popular, since it averages over 1 million visits and 12.9 million page views per month. Ticketmaster pointed out that a link to the popular Ticketmaster site may result in increased hits on the linking site (not the Ticketmaster site), and thus lead to increased advertising revenue (often generated by the number of hits).

3.5.1 Microsoft's site linked to the extremely popular Ticketmaster site

One of Microsoft's city guide websites "seattle.sidewalk.com" contained numerous links to Ticketmaster's site. As a result of this, Ticketmaster claimed that Microsoft violated the federally registered trademarks and that Microsoft was a freerider, committing electronic piracy by utilizing the Ticketmaster site in order to generate more advertising revenue to itself. Ticketmaster claimed it was deprived of favorable advertising business and opportunities due to the hyperlinking performed by Microsoft. Ticketmaster feared that the hyperlinks could confuse the potential consumers and give them reason to falsely believe that Ticketmaster was associated with Microsoft in any way, or that the two websites were supporting each other.

On May 28, 1997, Microsoft replied²⁵ to Ticketmaster's complaint. Microsoft totally denied being a freerider, and stated that Ticketmaster's complaint was based upon pure fiction since Microsoft itself never accessed Ticketmaster's website at all. It was the Internet users that visited the Ticketmaster site. Microsoft claimed not to be a party between the Internet users and Ticketmaster. Microsoft merely provided the URL address in the shape of a link to any Internet user that demanded it.

3.5.2 The lawfulness of hypertext links

Microsoft had received revenue from the sale of advertising space (on the Microsoft website) in connection with the links to the Ticketmaster site, but denied that Ticketmaster had been deprived of favorable advertising business or opportunities. Microsoft said that if Ticketmaster did not desire all Internet users viewing the sites, it could have refused access to anyone. Since Microsoft wanted to inform the public where to purchase tickets, Ticketmaster's name had to be displayed on Microsoft's site. According to Microsoft, Ticketmaster's complaint raised the question whether the use of

²⁴ [Http://www.ljx.com/LJXfiles/ticketmaster/complaint.html](http://www.ljx.com/LJXfiles/ticketmaster/complaint.html) (971017)

²⁵ [Http://www.ljx.com/LJXfiles/ticketmaster/answer.html](http://www.ljx.com/LJXfiles/ticketmaster/answer.html) (971017)

hypertext links is lawful. Microsoft wanted the court to remove all the doubts concerning the free workings of the Internet. On June 23, 1997, Ticketmaster replied,²⁶ denying that it attacked the general use of hyperlinks, and that it was an unlawful use and misappropriation of Ticketmaster's property. This case is yet to be treated in court, and it may (hopefully) become the first U.S. hyperlinking case not settling out of court.

3.6 Shetland News

On 24 October 1996, Judge Lord Hamilton in Scotland gave a preliminary interdict (equal to injunction) to prevent the newspaper Shetland News from using hyperlinks on its website to the rival Shetland Times.²⁷ The Shetland News site (www.shetland-news.co.uk) displayed various news headlines originating from the Shetland Times site (www.shetland-times.co.uk). These headlines consisted of hypertext links, that linked "deep" into the Shetland Times site. The main front page of the Shetland Times site was bypassed, as well as all advertising on it. The Shetland Times argued that such behavior constituted copyright infringement. The judge granted interim interdict, since the Shetland News would not suffer any major loss if prevented from hyperlinking to the Shetland Times sites. Perhaps the Shetland News site would be less interesting without the links to the Shetland Times and receive fewer hits, which could lead to loss of advertising revenue, in the long run.

One may argue that the Shetland Times does not suffer any harm when being the subject linked to. This may be true, but one should not forget that the linking might result in a loss of advertising revenue, since the front pages are bypassed. When it comes to intellectual property, there are pride and possessive feelings involved as well. It is completely understandable that authors detest seeing their work being utilized without compensation.

3.6.1 The interim injunction is not the death of hyperlinking in the U.K.

The main question in the case was whether hyperlinks are considered lawful. The interim injunction given by Judge Lord Hamilton should not be seen as the death of hyperlinking, since all the court considers in such a situation, is whether there is an issue to be tried and the balance of convenience. The questions concerning hyperlinking and whether a publisher on the Internet retains copyright in any material once it is published on the Internet, remains.²⁸

²⁶ [Http://www.ljx.com/LJXfiles/ticketmaster/reply.html](http://www.ljx.com/LJXfiles/ticketmaster/reply.html) (971017)

²⁷ [Http://www.shetland-news.co.uk/opinion.html](http://www.shetland-news.co.uk/opinion.html) (971006)

²⁸ *The Internet Copyright Case and its implications for users of the WWW*, by Professor Charles Oppenheim, Dec.6, 1996. [Http://www.shetland-news.co.uk/editorial/profopp1.htm](http://www.shetland-news.co.uk/editorial/profopp1.htm) (970715)

3.6.2 Newspaper headlines on a website may enjoy copyright

In the Shetland News case, only the URLs and the titles of the articles were actually copied, and therefore the Shetland Times had to prove that the URLs and the headlines were literary works worthy of copyright protection. According to Professor Charles Oppenheim, the courts in the United Kingdom very seldom consider copying or quoting parts of a sentence, or a single word as a copyright infringement.²⁹ This leads to the question whether single sentences, like in this case, a newspaper headline, could enjoy copyright. Professor Charles Oppenheim doubted that this could be the case, due to the absence of uniqueness and originality of the copied sentences, but he did not totally dismiss the idea that they could enjoy copyright.

3.6.3 URL may enjoy copyright

In the United Kingdom, it is not possible to have a single fact protected by copyright, and one could argue that the URLs are merely addresses, i.e. facts, and not worthy of copyright protection. Compilations of facts, however, could enjoy such protection. Professor Charles Oppenheim found it unlikely that the copying of the URLs in this case would be considered a copyright infringement, since only a few URLs were copied.³⁰

3.6.4 Fair dealing and implied license when copying URLs and news headlines

If a court would find the materials that was linked to copyrightable, the next question, according to Professor Charles Oppenheim, is whether the Shetland News was allowed to copy under the "fair dealing" doctrine or if any implied license to copy existed. He stated that in the United Kingdom, newspapers generally can copy from each other under this doctrine, due to the freedom of speech. Concerning an implied license, Professor Charles Oppenheim argued that by displaying information on a site on the World Wide Web, one must accept others linking to it, since linking is the core of the World Wide Web's construction and success. Oppenheim succumbs to the opinion that permission to link is granted by implication due to the mere fact that the site exists on the net. Professor Charles Oppenheim declared that if the Shetland Times would win the case, this would function as a barrier to the further development of the Internet in the United Kingdom. Sites overseas would not be affected by such an outcome he wrote.³¹

²⁹ [Http://www.shetland-news.co.uk/editorial/profopp1.htm](http://www.shetland-news.co.uk/editorial/profopp1.htm) (970715)

³⁰ *The Internet Copyright Case and its implications for users of the WWW*, by Professor Charles Oppenheim, Dec.6, 1996. [Http://www.shetland-news.co.uk/editorial/profopp1.htm](http://www.shetland-news.co.uk/editorial/profopp1.htm) (970715)

³¹ *The Internet Copyright Case and its implications for users of the WWW*, by Professor Charles Oppenheim, Dec.6, 1996. [Http://www.shetland-news.co.uk/editorial/profopp1.htm](http://www.shetland-news.co.uk/editorial/profopp1.htm) (970715)

3.6.5 Settlement reached in November 1997

The court unfortunately never tried the case, since the parties settled outside the courtroom on November 11, 1997. Under the settlement, the Shetland News was granted permission to link to the Shetland Times' headlines, but had to label individual articles as "A Shetland Times Story."³² Shetland News also agreed to display a button with the Shetland Times' logo that links to the newspaper's "front" homepage and not deep into its' website system.

3.7 Hypertexts in a Swedish perspective: Making a link is not equivalent of producing a copy of the material linked to

In Sweden, as far as I understand, there still do not exist any cases involving hyperlinking, but there are rules that might be applicable. According to Mr. Carlén-Wendels, a lawyer specialized in the field of IT, there do not exist any Swedish rules prohibiting hypertext links,³³ since solely producing a link is not considered equivalent of producing a copy. As the HTML code is written in the source of the web document, no copy is made, according to Mr. Carlén-Wendels. However, the user produces a copy (in his computer) once he *follows* the link. Not even a large protected photograph in the shape of an IMG should be considered infringement, since no copy is produced by the web-editor. When the user visits the site, a copy is produced and displayed on the site automatically. It is the user that unintentionally triggers the copying by visiting the site. The user is probably unaware of the fact that he/she produces a copy of a protected photograph. Even though one may argue that the user infringes upon copyrights by producing a copy, it would most certain be considered lawful according to the Swedish "private use doctrine".³⁴ It *may* be illegal if one considers the situation as infringement of the developer's right of delivery or performance, but this is uncertain at the moment. If the link consist of a protected trademark logo, the Swedish law³⁵ is applicable when the mark is used.³⁶

According to Swedish law, a traditional HREF link, written in a neutral font without displaying any logos or trademarks should not be considered an infringement. However, if a link consists of parts of the linked-to-site's content (text, not pictures), it may constitute infringement, but it may on the other hand be legal due to the right to quote.³⁷ The Swedish right to quote is, nonetheless, dependent upon moral and ethics.³⁸ Whether it would be moral

³² [Http://www.news.com/News/Item/0,4,16280,00.html?dtn.head](http://www.news.com/News/Item/0,4,16280,00.html?dtn.head) (971212)

³³ *Lag och rätt på Internet*, Thomas Carlén-Wendels, page 95.

³⁴ Lag (1960:729) om upphovrätt till litterära och konstnärliga verk, 1:12.

³⁵ Varumärkeslag (1960:644)

³⁶ *Lag och rätt på Internet*, Thomas Carlén-Wendels, page 95.

³⁷ Lag (1960:729) om upphovrätt till litterära och konstnärliga verk, 1:22.

³⁸ "God sed" in Swedish.

or not to quote the linked site in the linking site is uncertain. However, it may be possible to define the text describing the content of the linked-to-site, as an ordinary summary or review. Writing a brief summary explaining the content of the linked site is most likely lawful.³⁹ This of course, requires that the linker does not simply copy the text, or write too resembling. The linker should write a summary with his/her own words in order to avoid being subject to the regulations concerning quotations. This may not always be an easy task.

³⁹ *Lärobok i Immaterialrätt*, Kocktvedgaard and Levin, , page 158.

4 Caching

Caching is an operation of storing something in a place of storage. Caching in the world of computers is possible at multiple levels. In order to view a document on the screen it is necessary that a "copy" of that document is loaded into the Random Access Memory (RAM). If no copy is made in the RAM, nothing will be displayed on the user's monitor. When a computer browses the web, a plethora of information, such as recently visited web pages, pictures and texts, are stored locally on the computer's harddrive as well as in the computer's RAM. Often the browser creates a map called "cache" in the computer's directory in the explorer. This map contains fragments of visited sites, but it should not be confused with the caching taking place in the RAM. If the computer is switched off, only the information stored on the harddrive will remain. The information stored in the RAM will be lost forever.

How does the local caching work? If a person using Netscape Navigator for instance, wishes to retrieve a page recently visited, it is possible to press the "back" button in order to do so. The computer is then likely to display a page that is stored in the RAM instead of displaying a "new" copy of the page.⁴⁰ This can easily be demonstrated by closing down the Internet connection after browsing, while keeping the Netscape⁴¹ window active. Even though the user is off-line and the computer has no connection with the network, it is still possible to re-visit some of the sites the user visited, as he/she was on-line. These sites have been stored locally in the RAM, and fragments such as pictures etc. have been stored in the cache file on the harddrive. Once the computer is switched off, all the information in the RAM will be lost. The information stored in the cache file, however, is still intact after the computer has been switched off, but is insufficient in order to re-visit the sites off-line, since the cache-file mainly consists of fragments from the sites. In a normal browser, the user can easily decide the size of the memory cache and the disk cache when setting the network preferences. The size of the memory cache is, however, limited by the amount of RAM the computer is equipped with and the disk cache is limited by the amount of MB the harddrive contains.

4.1 Caching is sometimes considered a copyright infringement

Some people argue that the copy made in the RAM is a copy that can be juxtaposed to any other form of copy, and therefore RAM-copies could infringe copyrights. How could a copy in the RAM be sufficiently fixed in order to constitute a copy? According to Swedish law, a copy is made if the

⁴⁰ This procedure saves time for the user and relieves unnecessary congestion from the infrastructure.

⁴¹ Or another equivalent browser such as Microsoft's Internet Explorer.

work is transferred to a device through which it can be reproduced and displayed.⁴² Once the computer is switched off, the copy does not exist any more, but until then, the copy can be reproduced and displayed forever. I believe that such a copy would be legal under the fair use doctrine.⁴³ This doctrine in Sweden does not include computer programs though. The EU makes no distinction between temporary copies and permanent copies, as an act of reproduction.⁴⁴

4.2 Legal considerations concerning browsing

When users surf the Internet, browsers⁴⁵ are used in order to enable connection to all the various sites available. The phenomenon of caching is vital to the art of browsing, as described above. As the user ploughs through the available posted information in Cyberspace, the computer makes copies of the visited material in the RAM, in order to display it on the user's monitor. If no copies of the material were made into the RAM, nothing from remote sites would have been exposed to the user at all. Some argue that browsing is illegal due to the copying of posted protected material into the RAM, and thus the whole concept of surfing the net would be unlawful. One could argue that businesses and persons setting up public-access websites (sites not protected by passwords or other forms of security), implicitly agrees to let users enter, study and explore the site. If there exists an implied license to enter and explore a site, such a license would naturally include the copying of material into the RAM. If not, why would anyone go through the process of setting up a website if nobody can ever see it?

4.3 The increasing usage of passwords and user IDs supports the existence of an implied license to visit public-access sites

Today many sites require personal passwords and user IDs in order to enter, which further supports the existence of an implied license for web users. It has been argued that the fact that websites consist of intellectual property, not real property, does not hinder an implied license to visit, and consequently make a copy into the RAM as well.⁴⁶

The question of implied licenses is very interesting. Could one extend this idea and argue that businesses and persons implicitly agree to more, such as

⁴² Lag (1960:729) om Upphovsrätt till litterära och konstnärliga verk 2:2.

⁴³ Lag (1960:729) om Upphovsrätt till litterära och konstnärliga verk 2:12.

⁴⁴ *Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society*, Brussels, 10.12.1997. COM(97)628 final, page 37.

⁴⁵ The two most common browsing tools at this point in time are Netscape Navigator/Communicator and Microsoft Internet Explorer.

⁴⁶ *CyberLaw – The law of the Internet*, by Jonathan Rosenoer, page 10.

downloading of the posted material into a personal storage place, simply by setting up a site?⁴⁷

4.4 MAI Systems Corporation v. Peak Computer Inc.⁴⁸

In the U.S., there exist a few cases concerning the infected RAM issue. In the widely criticized case *MAI Systems Corporation v. Peak Computer Inc.*, MAI, a computer manufacturer, sued Peak, an independent service organization (ISO) servicing MAI computers for more than one hundred clients. MAI claimed that every time Peak serviced a MAI computer, parts of the MAI system software were copied into the RAM and that these copies violated MAI's copyright. The MAI software is an operating system software, which is one of the vital programs needed in order to run any other programs on MAI computers.

4.4.1 A copy stored in the RAM is considered a fixed copy under the Copyright Act

As Peak conducted routine maintenance and emergency repairs, it was often necessary for Peak technicians⁴⁹ to operate the computers, and thus starting up the operating system software in order to be able to see if the machines were functioning and operating as they should. In the case it was indisputable that if a computer is switched on, the operating system is loaded into the computer's RAM. Peak argued that the loading of copyrighted software did not constitute copyright infringement since the copy created in the RAM was not "fixed". The court defined RAM as a computer component in which data and computer programs can be temporarily recorded, until the computer is switched off. However, the court did not find any evidence showing that a copy created in the RAM would not be of a fixed nature, and stated that copies made in the RAM are "fixed" and qualify as copies under the Copyright Act.

It is very interesting that both the District Court and the Court of Appeal accepted MAI's argument. It was stated that copying for purposes of copyright law occurs when a computer program is transferred from a permanent storage device to a computer's RAM. It was shown that the work created in the RAM was "...sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than

⁴⁷ *Internet Technology makes it hard to protect a copyright*, Inside Business July 1997, by Kristen Caldwell. [Http:// www.hunton.com/in0797ib.htm](http://www.hunton.com/in0797ib.htm) (971015)

⁴⁸ *MAI Systems Corporation v. Peak Computer Inc.*, 991 F.2d 511 (9th Cir.1993) [Http://www.law.seattleu.edu/chonm/Cases/mai.html](http://www.law.seattleu.edu/chonm/Cases/mai.html) (971026)

⁴⁹ Even though it has no relevance in the case, it may be interesting to note that a few MAI employees left MAI and were hired by Peak.

transitory duration.”⁵⁰ This led to a situation where Peak Computer, would be liable to copyright infringement every time any of its servicemen turned on a computer with MAI software on it, in order to service the equipment. It is worth noting that since Peak did not raise fair use as a defense, the court never considered this issue.

4.4.2 The rightful possessor of a computer program cannot authorize a third party to make a copy

How could the courts reach such a bizarre decision? One should keep in mind, that before the Copyright Act⁵¹ was enacted, the Commission on New Technological Uses of Copyrighted Works, known as the CONTU Commission⁵² recommended two words in section 117 to be replaced. The CONTU Commission suggested a wording stating that it would not be an infringement if the *rightful possessor* of a copy of a computer program authorized the making of another copy under certain circumstances. This would have facilitated for persons with only software licenses (software is generally licensed, not sold nowadays⁵³), to authorize third parties, such as Peak Computer Inc. to service their computers and help them when the computers are stuck. Congress did not listen to the CONTU Commission and used the word *owner*, instead of *rightful possessor*, which (with help from the courts) has led to the situation where no other company than the software copyright holder is allowed to turn on the computer in order to service it. Some argue that the use of the word *owner* was unnecessary since owners did not need additional protection.⁵⁴ An owner would be able to copy and do whatever he wanted with the program he developed anyway. Some argue that the distinction between copying and using has been diluted as a result of the case and the wording of the section 117 of the Copyright Act.⁵⁵

4.5 Triad Systems Corp. v. Southeastern

⁵⁰ *MAI Systems Corporation v. Peak Computer Inc.*, 991 F.2d 511 (9th Cir.1993) at /11. (17 U.S.C. s 101)

[Http://www.law.seattleu.edu/chonm/Cases/mai.html](http://www.law.seattleu.edu/chonm/Cases/mai.html) (971026)

⁵¹ The Copyright Act §117 Limitations on exclusive rights: Computer programs. [Http://www.sgpdlaw.com/software_copyright/part1.html#117](http://www.sgpdlaw.com/software_copyright/part1.html#117) (971025)

⁵² *Turning On and Turning Off: Can Merely Turning On a Computer Constitute Copyright Infringement? In the Ninth Circuit, Yes*, by Ronald S. Katz and Janet Arnold Hart, The Recorder Intellectual Property Supplement, Autumn 1995. [Http://www.coudert.com/turnon.htm](http://www.coudert.com/turnon.htm) (971022).

⁵³ *Ninth Circuit Uses Copyright Law to Slam Independent Service Organizations*, LGU Technology Law Bulletin, July 1993. [Http://www.lgu.com/cr47.htm](http://www.lgu.com/cr47.htm) (971024)

⁵⁴ *Turning On and Turning Off: Can Merely Turning On a Computer Constitute Copyright Infringement? In the Ninth Circuit, Yes*, by Ronald S. Katz and Janet Arnold Hart, The Recorder Intellectual Property Supplement, Autumn 1995. [Http://www.coudert.com/turnon.htm](http://www.coudert.com/turnon.htm) (971022).

⁵⁵ *Ibid.*

Express Co.⁵⁶

A similar case brought the question one step further by including the fair use doctrine into the matter. The facts are similar to those in *MAI v. Peak*. Southeastern is an ISO that services Triad computers. The license terms used by Triad, prohibited reproduction or use of the software by third parties. When Southeastern technicians serviced Triad computers, they had to make copies of the operating system, as well as of the service and diagnostic software in the RAM. Because of this, Triad sued Southeastern in April 1992, claiming copyright infringement. Southeastern lost in the district court⁵⁷ and was prohibited from servicing Triad computer systems.

4.5.1 Defense of fair use rejected

The case was tried again in the 9th circuit in 1995. Southeastern raised fair use as a defense but the court rejected this. The court cited the Copyright Act §107,⁵⁸ which sets out four main factors determining whether a use is considered fair use. Firstly, it is necessary to determine the purpose and character of the use. Is it of a commercial nature or is it for nonprofit educational purposes? Secondly, one must decide the nature of the copyrighted work. Thirdly, the amount or quantity of the copyrighted material used must be decided. Is it all of it, or only a portion? Fourth, the effect of the use upon the potential market must be determined. Has the value of the copyrighted work diminished as a result of the use?

The ninth Circuit concluded that Southeastern had developed nothing of its own and that the copies made by Southeastern while servicing Triad computers diminished the value of Triad's copyright. Since Triad invented, developed, and marketed its software in order to be able to service Triad computers, Southeastern was "...getting a free ride when it uses that software to perform precisely the same service."⁵⁹ The fair use was rejected. Southeastern should pay license fees to Triad.

⁵⁶ *Triad Systems Corporation v. Southeastern Express Co.*, 64 F.3d 1330 (9th Cir.1995)

[Http://www.softwareindustry.org/software/issues/docs-htm/triad-1.html](http://www.softwareindustry.org/software/issues/docs-htm/triad-1.html)

⁵⁷ [Http://www.law.seattleu.edu/chonm/Cases/triad.html](http://www.law.seattleu.edu/chonm/Cases/triad.html) (District court)

⁵⁸ *Triad v. Southeastern* at [14] p.10907. (17 U.S.C. S 107. Text can be found at

<http://www.law.cornell.edu/uscode/17/107.shtml>)

⁵⁹ At [5] p. 10908. *Triad Systems Corporation v. Southeastern Express Co.*, 64 F.3d 1330 (9th Cir.1995)

[Http://www.softwareindustry.org/software/issues/docs-htm/triad-1.html](http://www.softwareindustry.org/software/issues/docs-htm/triad-1.html)

4.6 Summary

Presumably most people succumb to the opinion that caching is one of the basic cornerstones of the Internet. In order to browse, or even see documents, one must allow the computer to produce copies in the RAM and on the harddrive. Even though this is natural and obvious to most Internet users, one should not forget that courts such as the MAI court and the Triad court stated that copies in the RAM technically qualify as copies within the meaning of the law. If one cannot claim that it is lawful to produce temporary copies in the ram, or relatively permanent copies on the harddrive, due to the private use doctrine (and fair use doctrine as well), the whole Internet community could be infringing upon copyrights all the time. However, I believe such copies are lawful, due to the private use doctrine. If the private use doctrine would not be applicable, one could argue that implied licenses allow such copying. The question of implied licenses seems to become clearer and clearer, due to the increased usage of passwords as well as user IDs. Perhaps one can assume that when a site is a public-access site, there always exists an implied license to visit the site, and thus produce the necessary copies in order to view the posted information?

5 Proxycaching

When caching occurs at the server level, it is often referred to as proxycaching. Companies, which store the most frequently requested sites on their servers, such as AOL and CompuServe, gain from proxycaching. Copies of the most popular sites are cached on secondary servers in order to avoid servers braking down due to overload. As a result of proxycaching, the requested data will be delivered faster to a greater number of users and with as few interruptions as possible.

5.1 The legal dilemma of proxycaching

Website owners may not be able to control the data being delivered to those users requesting the site, when additional copies of the site are stored on remote servers. If the website owner updates the information on his/her site, it is not certain that the various proxycached copies are updated as well. The result following this would be that some users would access the updated version, while others access the proxycached old version. Suppose that the website owner discovers that some information posted on the site is illegal or incorrect, and removes it as fast as possible in order to avoid legal repercussions. Even if the harmful information is removed from the original site, it may very well still be posted on the proxycached version until the company providing the server decides to refresh the site.⁶⁰ The users receiving the old cached version may be offended or base certain actions upon the incorrect information and file a suit, since they believe that they are receiving up-to-date information. Another problem may arise if the site owner has contract with advertisers who bought space on the site. Often the banner ads change regularly and advertisers pay for certain amount of time that the banner is displayed. If the site is proxycached, the banner ad may not be displayed at all, or much longer than the contract says.⁶¹ If the companies performing the proxycaching would refresh the proxycached sites extremely often, no situation as described above would probably occur.

5.1.1 Page impressions

Another problem may arise for the site owner. He/she may not be able to keep track of the number of users that visit the site, and this may have negative consequences when advertisers choose where in Cyberspace to place their ads, or if the site owner charges advertisers based upon the number of hits. If the site is proxycached on several servers, it may be troublesome to keep track of all the users visiting the various copies of the same document. Professor Eric Schlachter mentioned "page impressions" as an example of when proxycaching leads to difficulties in charging

⁶⁰ *Cache-22: Copying and storing Web pages is vital to the Internet's survival - but is it legal?* By Eric Schlachter. Intellectual Property Magazine Summer 1996. [Http://www.ipmag.com/schlacht.htm](http://www.ipmag.com/schlacht.htm)

⁶¹ Ibid.

advertisers. Page impression is when the charge is based upon the number of times the banner ads are exposed to users. If the site is proxycached, it is impossible to tell how many users that were exposed to the banner, and thus more difficult to charge advertisers for the impressions done from the cache.

5.1.2 A proxycached site constitutes a copy

The process of caching a site and storing it on a remote server somewhere is most likely equivalent of producing a copy. If no consent is given from the site owner, it could in certain circumstances constitute copyright infringement. Professor Eric Schlachter stated that the companies using proxycaching, may be liable for copyright infringement "...both of the Web sites being cached, and of third parties if the cached pages have infringed others' copyrights."⁶²

5.1.3 Fair use to utilize proxycaching

As in *Triad v. Southeastern*, it may be possible to claim that proxycaching would constitute fair use. If one looks at the Copyright Act §107, the four factors discussed above must be considered. The purpose of the use of proxycaching would be to speed up connections in order to get the most out of the present infrastructure. Regarding the nature of the copyrighted work, I succumb to the opinion of Professor Eric Schlachter, that all material posted on the Internet, is considered published (for purposes of copyright). Regarding the amount of the copyrighted work that is used when copied to a remote server, I believe that almost the whole content of the site is copied. However, I do believe that some IMG links are not part of the proxycaching, and therefore should not be included in the amount of the work that is considered used. The important factor is that almost the whole work is copied. Concerning the effect upon the potential market, I again, succumb to Professor Eric Schlachter's opinion, that mostly sites containing advertisements in any way are disturbed by the proxycaching. It is difficult to decide what a potential market is for a plain site that does not contain any advertisements. One can only speculate how a court would decide in a matter like this.

5.2 Proxycaching in a Swedish legal perspective

According to Swedish law⁶³ only the author has the right to copy his work. If the work is posted on a database or equivalent, it is considered as copying, if the work can be reproduced by such an act.⁶⁴ I do not consider the copying taking place in a proxycaching situation being much different from the

⁶² *Cache-22: Copying and storing Web pages is vital to the Internet's survival - but is it legal?* By Eric Schlachter. Intellectual Property Magazine Summer 1996. [Http://www.ipmag.com/schlacht.htm](http://www.ipmag.com/schlacht.htm)

⁶³ Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk 8§.

⁶⁴ Dag Mattson in Karnov 1996/97, page 919 at note 14.

copying taking place when posting a work on a database where it may be reproduced. There are many similarities in copying a complete work to a database, and copying a complete work to a server. The work may be viewed and reproduced in either way. Sometimes a compilation of hyperlinks on a webpage is considered a compilation of facts,⁶⁵ which enjoy copyright. If such a compilation or any other copyrighted work is copied onto a second server in order to perform proxycaching, I am of the opinion that it is a question of copying within the meaning of the Swedish law.⁶⁶ Proxycaching would therefore not be legal according to Swedish law. Some may argue that this copying would be legal due to the “private use doctrine”⁶⁷, but I believe that reproducing a website that becomes available to an infinite number of users should not be considered private use. One could argue, as in the case with normal caching, that by posting material on a site, the site owners implicitly agree to allow such copies to be made, since it is almost a matter of normal procedure in Cyberspace nowadays. The risk that sites will be victims of congestion and break down is diminished when additional copies are stored on different servers. However, since the site owners tend to loose control over their sites after being proxycached, one could argue that it is not at all certain that there exists an implied license to proxycache.

5.3 Summary

The problems which come with the creation of several versions of the same website (when proxycaching), could easily be avoided if the proxycached websites are updated on a daily basis. This is technically possible, but whether it is economical for the companies performing the proxycaching is burdensome to tell. When a site is proxycached, a copy of the work is produced, and since the copy is available to a large number of users, it should not be lawful according to any private use or fair use doctrine. It is not at all certain that there exists an implied license to produce copies of the websites on a remote server, since site owners tend to loose control over their sites.

⁶⁵ Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk 5§.

⁶⁶ Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk.

⁶⁷ Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk 12§.

6 Domain Names

6.1 Internet Protocol addresses

It is in Cyberspace, as it is in the real world, that people and organizations need names and addresses in order to be contacted and identified. A company without a name would probably not go very far. Who would trust it? In Cyberspace, Internet Protocol addresses (IP addresses) are used in order to locate and distinguish all computers connected to the Internet. IP addresses consist of digits divided into several parts separated by periods. A typical IP address could look like the following: 123.45.67.890. IP addresses contain a network portion beginning on the left and a local portion ending on the right.⁶⁸

6.2 Top level designators

Since it is bothersome to remember miscellaneous combinations of digits, there exist mnemonic designations⁶⁹, called domain names that are connected to the IP addresses, which makes the whole on-line system user-friendlier. Most Internet applications will automatically, when given a domain name, contact the corresponding IP address in order to retrieve the requested site. The Domain Name Service (DNS) does this through an invisible conversion process.⁷⁰ An example of a complete domain name could be www.sjobeck.com. Domain names are, as the IP numbers, divided into parts separated by periods. The first name from the right is the top-level designator (TLD), or primary level domain name. There exist various types of TLDs at the moment.⁷¹ Country codes are one example. These represent the country (two letters) to which the address belongs. Currently, there exists over 180 two-letter country code TLDs. For instance, .com (commercial), .se (Sweden), .de (Germany), .uk (United Kingdom), .be (Belgium) etc. In the U.S., certain TLDs (three letters) are reserved for the military (.mil),

⁶⁸ *Trademarks Along the Infobahn: A first Look at the Emerging Law of Cybermarks*, by Dan L. Burk, April 10, 1995, 1Rich. J.L & Tech.1(1995). [Http://www.nlc-bnc.ca/ifla/documents/infopol/copyright/burd1.htm](http://www.nlc-bnc.ca/ifla/documents/infopol/copyright/burd1.htm) (970725)

⁶⁹ *Tension Between Paralell Universes: Trademarks clash with domain names as business identify moves onto the Internet*, by Mark F. Radcliffe and Maureen S. Dorney. Intellectual Property Magazine, winter 1996. [Http://www.ipmag.com/radcliff.htm](http://www.ipmag.com/radcliff.htm) (970716)

⁷⁰ *Trademarks Along the Infobahn: A first Look at the Emerging Law of Cybermarks*, by Dan L. Burk, April 10, 1995, 1Rich. J.L & Tech.1(1995). [Http://www.nlc-bnc.ca/ifla/documents/infopol/copyright/burd1.htm](http://www.nlc-bnc.ca/ifla/documents/infopol/copyright/burd1.htm) (970725)

⁷¹ There is a proposal advanced by the International Ad Hoc Committee on the Internet (IAHC) in its final report from Feb.4, 1997 to add seven new gTLDs (or more).

educational institutions (.edu) and governmental agencies (.gov). Also, there exists generic TLDs, often referred to as gTLDs. These can be used by anyone from any country in the world (.com, .org, and .net). Another TLD (.int) is reserved for international treaty organizations.⁷²

6.3 Secondary level designators

The secondary level (SLD) of the Internet domain name is an extremely controversial issue all over the world, since only one registration of a specific name is allowed. There can be an unlimited number of different SLDs in each TLD, but there can be only one of each specific SLD in each TLD. If “sjobeck” is registered as a SLD, nobody else can use that exact word as a SLD together with the same TLD. Only modified variations of “sjobeck” can be used within the same TLD. For example, “sjobeck1” would most likely be accepted, since it is not the very same phrase or word. Likelihood of confusion does not matter.⁷³

6.4 The need for a universal domain directory service

However, companies strive to have the user-friendliest URL possible, since nobody can remember various combinations of digits and letters. Sometimes a domain name has a third-level domain name, but this is not mandatory.⁷⁴ Generally speaking, domain names are not very difficult to obtain, but receiving a domain name very closely related to a company’s own trademark, logotype, service mark, business mark or product name may be troublesome. Users often search for the company’s name (together with www and the ending .com) in order to find the company they are searching for.⁷⁵ Most companies struggle to have a domain name that is easy to remember, due to the lack of a universal directory service that allows users to find the domain name of any trademark holder in the world. A very long and complicated URL may function as a deterrent upon lazy users. The battle for the most natural and simple domain names has given rise to numerous trademark disputes around the globe. WIPO is of the opinion that by creating a universal directory, the pressure upon the domain name system

⁷² WIPO, Issues relating to trademarks and Internet domain names. First session, Geneva, May 26 to 30, 1997.

[Http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm](http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm)

⁷³ *Revised Rules Govern Domain-Name Disputes*, by Seyamack Kouretchian, The National Law Journal, Oct 28, 1996.

[Http://www.ljx.com/Internet/filetm.html](http://www.ljx.com/Internet/filetm.html) (971104)

⁷⁴ There must always be at least two parts. An example of a thirdlevel domain name could be sjobeck.co.uk. Domain name levels are counted from right to left.

⁷⁵ WIPO, Issues relating to trademarks and Internet domain names. First session, Geneva, May 26 to 30, 1997.

[Http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm](http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm)

would decline, since companies would then be less reluctant towards using “not memorable” domain names.⁷⁶

Sometimes several companies with the same registered trademark (perhaps in different countries or concerning different kind of goods) desire the same URL. Only one can have the preferred trademark registered as a SLD.

6.5 Registering domain names in the United States

In the U.S., domain names are assigned by the Internet Assigned Numbers Authority (IANA), which has delegated most of the duties to Internet Network Information Center (InterNIC) which is operated by Network Solutions, Inc (NSI). NSI has a contract to operate InterNIC through September 1998.⁷⁷ InterNIC charges a fee (about \$100) per domain name registered. This payment will only cover the first two years. In addition, there is an annual maintenance cost (about \$50) of keeping a domain name registered.⁷⁸ The second-level domain names have been distributed on a so-called “first come, first served” basis until September 1996. After series of cybersquatting, NSI chose to change this policy.⁷⁹

6.5.1 The domain name dispute policy

The applicants must, nowadays, certify to the best of their knowledge that they are not violating any other entity’s trademark rights and that they have the legal right to use the proposed names. InterNIC has reserved the right to revoke an assigned domain name upon thirty days written notice.⁸⁰ Because NSI was made the target of several lawsuits, special registration policies were formed.⁸¹ InterNIC developed a widely debated domain name dispute policy which has been revised a number of times since 1995. NSI has taken the position that it is not competent enough to resolve all domain name

⁷⁶ Ibid.

⁷⁷ *The Name Trade: How to deal for a domain*, by Jefferson Scher, Intellectual Property Magazine, December 1996.
[Http://www.ipmag.com/scher.htm](http://www.ipmag.com/scher.htm) (970716)

⁷⁸ *Tension Between Paralell Universes: Trademarks clash with domain names as business identify moves onto the Internet*, by Mark F. Radcliffe and Maureen S. Dorney. Intellectual Property Magazine, Winter 1996.
[Http://www.ipmag.com/radcliff.htm](http://www.ipmag.com/radcliff.htm) (970716)

⁷⁹ *The domain name currently called Prince*, by Douglas Hayward. Techwire 07/31/97.
[Http://techweb2.web.cerf.net/wire/news/jul/0731prince.htm](http://techweb2.web.cerf.net/wire/news/jul/0731prince.htm) (970801);
Revised Rules Govern Domain-Name Disputes, by Seyamack Kouretchian, The National Law Journal, Oct 28, 1996.
[Http://www.ljx.com/Internet\(filetm.html](http://www.ljx.com/Internet(filetm.html) (971104)

⁸⁰ Satterlee Stephens Burke & Burke LLP.
[Http://www.sbb.com/trademar.html](http://www.sbb.com/trademar.html) (971009)

⁸¹ *Cyberlaw: Issues in Internet Commerce*, by Thomas E. Jensen.
[Http://www.cyberlaw.com/issues.htm](http://www.cyberlaw.com/issues.htm) (970724)

disputes in a righteous way, and therefore those matters are to be solved privately or in courts. However, in the event of a dispute, certain procedures should be followed. For instance, a trademark owner must send a letter to the domain name holder, containing a warning. If the warning letter and a certified copy of the trademark registration are sent to InterNIC, the domain name will be closed down after thirty days, awaiting the settlement of the dispute. This policy has caused domain name proprietors to protest. They claim that the NSI policy penalizes site operators charged with trademark infringement, before any actual infringement has been proven.⁸² NSI Internet business manager David Graves defends the dispute policy, saying that there are several options available to domain registrants, such as changing the domain name, having the site deactivated, or resolving the matter in court.⁸³ If one has done nothing wrong or unlawful, such options seem quite burdensome and unfair.

6.6 Registering domain names in Sweden

In Europe, the registration of domain names is controlled by the “Resaux IP Européens” (Regional Internet Registry for Europe) Network Coordination Centre (RIPE NCC). RIPE delegate the responsibility to national institutions, such as the “Swedish Kungliga Tekniska Högskolan Network Operation Centre/Internic.se” (KTHNOC). The “Informationstekniska Standardiseringen” (ITS) and its workgroup 12 (AG12) are responsible for setting up a policy and a framework of rules relating to domain names.⁸⁴ This policy requires that only companies, organizations, or authorities may register a domain name. Private persons may not do so. The domain name must be closely and uniquely linked to the official registered name used by the company in the “physical” world outside Cyberspace. In other words, in order to receive a certain domain name, there must exist a substantial genuine relationship to the name before sending in the application. A document proving such a relationship must be attached to the application. The Swedish rules concerning registration of domain names are quite stringent, in comparison to the corresponding American rules. There should not be a great amount of domain name disputes with the Swedish domain name system. However, one should not ignore the fact that two companies in different businesses may use the same trademark, and this could lead to disputes, since only one of the companies can use the trademark as a domain name with the TLD .se.⁸⁵ Suppose the insurance company “WASA” and the breadmaker “WASA” both want the domain “www.wasa.se”.⁸⁶ Who is entitled to the domain? Geographical names may not be used, unless the

⁸² *Domain name disputes: Preemptive Suits*, by Joanna Glasner. Law Journal EXTRA!, Sept. 17, 1997. [Http://www.ljx.com/ljxfiles/domainlaw.html](http://www.ljx.com/ljxfiles/domainlaw.html) (971012)

⁸³ Ibid.

⁸⁴ *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, p 106 and homepage of internic.se at [Http://www.internic.se](http://www.internic.se) (971104)

⁸⁵ *Praktisk IT-rätt*, by Agne Lindberg and Daniel Westman, page 27.

⁸⁶ This example is completely fictive, but the companies do exist.

company legally can claim the right to do so. Protected names, such as trademarks, may only be used by the rightful owners. However, trademarks may only be used if they represent the name of the organization, not if they represent a service, product or equivalent.⁸⁷ This circumstantial procedure may be bothersome, but it may hinder sinister cybersquatters.

6.7 Cybersquatting

Another problem is that of cybersquatting. Individuals deliberately register well-known trademarks in order to sell or lease them back to the rightful trademark owners in the future, if the companies decide to create a website. I believe this is a diminishing problem, since most companies have gone on-line by now. There have been a number of suits, especially in the U.S., relating to cybersquatting. In Europe there have been a number of suits, especially in the U.K., the Netherlands and Germany. One could say that the legal status of domain names is relatively uncertain. It is not decided yet, whether domain names are like trademarks, capable of being protected, or if they are similar to street addresses without protection.⁸⁸

6.7.1 Reasons why one ought to fight a cybersquatter

These people with questionable motives, who bargain for monetary settlements in order to release the domain names to the trademark owners, have caused a lot of anger and frustration among large well known companies during the last couple of years. If one detects that one's trademark is registered as a domain name by a cybersquatter, should one choose to fight him or simply let it be, especially if the trademark owner does not need the domain name? Except for the costs involved in fighting a cybersquatter, there may be several worthy reasons (relating to intellectual property issues) to fight a legal battle against a cybersquatter. If the company does not care about the cybersquatter's unauthorized continuous use of its trademark, as a domain name, this may dilute the strength of the trademark.⁸⁹ People may not associate the trademark to a certain product or company any longer if the cybersquatter's website is popular and frequently visited by numerous users. Also imagine if the domain name (that includes the unauthorized use of the company's trademark) is associated with immoral material, such as adult information, racist propaganda or equivalent. This could directly have a harmful effect on the company's reputation and goodwill.

⁸⁷ [Http://www.internic.se](http://www.internic.se) (971104)

⁸⁸ *Tension Between Paralell Universes: Trademarks clash with domain names as business identify moves onto the Internet*, by Mark F. Radcliffe and Maureen S. Dorney. Intellectual Property Magazine, Winter 1996. [Http://www.ipmag.com/radcliff.htm](http://www.ipmag.com/radcliff.htm) (970716)

⁸⁹ Satterlee Stephens Burke & Burke LLP. [Http://www.ssbb.com/trademar.html](http://www.ssbb.com/trademar.html) (971009)

6.7.2 Hostile takeover of trademark by cybersquatter

Another reason to fight a cybersquatter is that he/she may in the future claim that the trademark no longer is entitled to protection, since it has been used by other parties as a domain name, without any objection from the trademark owner.⁹⁰ An unregistered trademark may be entitled to protection, if it has been used and established for a long period of time.⁹¹ Suppose a cybersquatter is left alone for a long time. What if he/she starts a business with the “stolen” domain name and uses it for several years. It is not completely unlikely that the cybersquatter could be entitled to use the trademark due to the fact that the company never protested to the usage of the domain name.

6.8 Confusing domain names

Suppose a potential client types the name of a law firm (or other firm) in the URL, and discovers that the site is filled with very disturbing and unpleasant content? If it is not obvious that the site belongs to someone else, the user may be deceived. Even if it is obvious that the site does not belong to the company, the user may be doubtful and believe that the company supports, or has some kind of connection to the obscene site, since the name of the company is displayed in the URL. This kind of confusion has actually been the case with the domain name “internic.com”. Users sought registration for their domain names at a website with the above described domain name. They all thought that it was the official site of Network Solution’s InterNIC, and paid \$250 for a domain registration. However, the official InterNIC site has the domain “internic.net”, and charge \$100 for a domain name registration. Apparently, the phony company owning “intenic.com” registered the domain names for its “clients” at the cost of \$100 at the “real” InterNIC. This fake company seemingly made a profit of \$150 of every registrant believing that the site was the official InterNIC site, due to its confusing domain name.⁹²

6.9 Possible conflicts between domain names and trademarks

Much of the controversies about trademarks on the Internet concern the registration as well as the use of domain names. Trademark issues were not taken into account when registering domain names at first-come, first-served basis. This did, naturally, lead to various conflicts between the allocated domain names, and the existing intellectual property rights. Trademark law

⁹⁰ Ibid.

⁹¹ *Lärobok I Immaterialrätt*, by Koktvedgaard and Levin, page 297.

⁹² The Net: *Domain resellers confuses users*, by Janet Kornblum, July 9, 1997. [Http://www.news.com/news/item/o,4,12296,00.html?dtn.head\(971009\)](http://www.news.com/news/item/o,4,12296,00.html?dtn.head(971009))

permits that the same trademark is used for different types of goods.⁹³ A trademark may co-exist in different countries as well. However, on the Internet, there cannot exist two domain names spelled exactly the same way. Companies using the same trademark, operating in different fields or countries may have to fight to be able to use the trademark as a domain name.

The term “trademarks” does not include domain names, even though one may say that domain names are trademark-like by their nature.⁹⁴ Some may argue that domain names are very much like trademarks, and thus entitled to protection, and others may argue that domain names are more like street addresses, not to be protected or owned. It is almost indisputable that domain names are performing a similar role, in Cyberspace, as trademarks have played in traditional types of businesses.⁹⁵ Domain names are often used to identify a source of goods or services. WIPO has called for a discussion concerning issues mentioned above. For example, in the September memorandum, it says that the International Bureau has initiated a survey regarding under which conditions holders of domain names could obtain and maintain the registration of the domain name as a trademark.⁹⁶

6.10 Trademarks and domain names in Sweden

In the light of Swedish rules, domain names could in some cases be considered equal to trademarks. In Swedish law, the trademark is the link between a company and its customers. It could function as a source of origin, warranty of quality, as well as tool for individualizing the company.⁹⁷ If a trademark has existed for a long period of time, it may have an intrinsic value.

A trademark must be distinct and different from other trademarks in order to enjoy protection.⁹⁸ If only minor details separate a mark from another, it is not said to be distinct, since it resembles the primary mark. Registration as trademark in such a situation would therefore not be possible. If domain names would enjoy the same protection as trademarks, the same rules would apply to them. One could argue that a domain name, which is registered after another with merely a minor deviance from the first (such as a number

⁹³ For instance, Varumärkeslag (1960:644) 6§.

⁹⁴ WIPO Consultative meeting on trademarks and Internet domain names, First Session, Geneva, May 26 to 30, 1997.

[Http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm](http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm)

⁹⁵ INTA (International Trademark Association) “White Paper” - *The Intersection of Trademarks and Domain Names*, Feb 5, 1997, Version 1.0. [Http://plaz.interport.net/int/wpwhole.htm](http://plaz.interport.net/int/wpwhole.htm) (971121)

⁹⁶ WIPO, Consultative meeting on Trademarks and Internet Domain names, second session, Geneva, September 1 and 2, 1997.

[Http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_ii_2.htm](http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_ii_2.htm) (971025)

⁹⁷ *Lärobok I immaterialrätt*, Koktvedgaard and Levin, page 305.

⁹⁸ Varumärkeslag (1960:644) 2§ and 12§.

or single letter), would not be able to register as a domain name in Sweden. The first name, however, may be able to do so. For example, suppose a company registered the domain name “cyberburger” as a trademark. Perhaps this is distinct enough to enjoy protection as a registered trademark, but I am of the opinion that a second registration such as “cyberburgers” or “cyberburger1” would not be distinct enough to enjoy protection as registered trademarks. However, these domain names may after a lengthy period of time, be distinct due to the fact that they have been used and widely recognized.⁹⁹ They would at that point not qualify for registration, but perhaps for protection. Another question is whether they would be admitted to be used for such a long period at all. According to [internic.se](http://www.internic.se), only the respective owners may use protected trademarks, if the trademarks are the same as the name of the organization. As mentioned above, no trademarks related to names of products, services etc. can be registered as domain names in Sweden.¹⁰⁰ However, in the U.S., it is possible to register a trademark referring to a product, service etc. as a domain name as long as no trademark infringement is at hand.¹⁰¹

6.11 Domain names are not solely descriptive

If a mark is solely descriptive, it may not be registered as a trademark and enjoy protection. Could one argue that domain names in general are descriptive and not distinct at all? Can a domain name in itself be more than merely a descriptive phrase? I am of the opinion that it can, since a domain name can express originality, distinctiveness as well as give a hint of the content of the site. Special original combinations and combinations of words may enjoy protection. I believe that domain names can be registered as trademarks, if they fulfill the requirements expressed by the law. It may be worth to register a domain name as a trademark as fast as possible in order to avoid conflicts in the future.¹⁰²

6.12 Registering a trademark consisting of a gTLD

Some authors claim that domain names have nothing in common with trademarks, and should therefore not be able to enjoy trademark protection at all.¹⁰³ One argument is that some websites, such as “NBC.COM”, which are named after their domain addresses cannot be registered. The Patent and Trademarks Office (PTO) has said that “NBC” can be registered and enjoy protection, but the “.COM” part cannot. This is by some authors, seen as a

⁹⁹ Varumärkeslag (1960:644) 2§ (inarbetning).

¹⁰⁰ [Intrenic.se](http://www.internic.se). [Http://www.internic.se](http://www.internic.se) (971104)

¹⁰¹ *Your Handbook of Everyday Law*, by George Gordon Coughlin, Jr, page 338.

¹⁰² *Nätjuridik – Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 108.

¹⁰³ *Why Federal Trademark law does not protect Internet Domain names*, by Jeff Wilson. [Http://www.libraries.wayne.edu/~jlitman/pwilson.html](http://www.libraries.wayne.edu/~jlitman/pwilson.html) (971121)

sign supporting the argument that domain names are similar to addresses. It may very well be that the gTLDs, such as “.com”, are too common even to be part of a trademark, but I believe that the SLDs must be individual and distinct in order to be registered.

6.13 The possibilities of domain names infringing upon already existing trademarks and vice versa

Another question is whether domain names can infringe upon already existing trademarks and vice versa. Can solely the registration of a domain name be an act of infringement, if a domain name is the same as a registered trademark? If a company only offers its services on-line, providing information for example, the domain name could possibly be considered as a trademark. The domain name could fulfill the same function as a trademark. The use of the domain name would be treated in the same way as the use of a trademark.¹⁰⁴ If this would be the case, a domain name could possibly infringe upon an already existing trademark, if the type of business is the same, or if the distinctiveness of the trademark is diluted by the use of the domain name. Once the legal status of domain names is more certain around the globe, it will be easier to determine whether domain names infringe upon trademarks and vice versa. Some cases, such as the Roadrunner case described below, suggest that trademarks and domain names can infringe upon each other.

6.14 Domain name infringements and disputes

Since domain names have grown to become an important issue to most companies today, there have been many disputes relating to this issue. There exist numerous disputes concerning domain names and trademarks, especially in the U.S.¹⁰⁵ Many of the cases raise extremely interesting questions relating to the whole concept of domain names, but “unfortunately” many of the parties choose to settle their domain and trademark disputes outside the courtrooms in order to keep the costs and publicity down. It might be good for the parties involved settling quietly, but it does not help clarifying or improving the regulatory evolution of Cyberspace law.

¹⁰⁴ *Nätjuridik – Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 111.

¹⁰⁵ One of the most publicized early disputes was between Josh Quittner and McDonald’s. Quittner discovered that McDonald’s had not registered their trademark as a domain name, and did so himself. At first McDonald’s did not care. In addition to this, he registered an e-mail address “ronald@mcdonalds.com”. He wrote an article about his endeavors on his site. McDonald’s had to pay \$3,500 to a public school so that it could afford computers, in order to receive the domain name.

6.15 MTV Networks v. Adam Curry¹⁰⁶

One of the early disputes concerning domain names and trademarks is *MTV v. Curry*. Adam Curry served as a video disc jockey (VJ) for MTV. During his employment time as a VJ at MTV, he organized a website with the domain name MTV (www.mtv.com). He registered the domain name in his own name. In June 1993 Curry discussed the site with the MTV Vice President Matthew Farber, who apparently indicated that Curry was free to continue the development of the Internet website at his own expense. MTV was not interested in any joint venture at all, and did not object to the fact that Curry registered the domain name “mtv.com”. During the same year, Curry left MTV, but Curry continued to develop mtv.com at his own expense another half year until January 19, 1994, when MTV formally requested that Curry should cease using the “mtv.com” domain. At this point in time, his website had been accessed by millions of users worldwide. Since Curry had registered the domain name personally, MTV could not control the site.

The dispute was moved to court as MTV sued Curry for trademark infringement and unfair competition. Curry argued that MTV used Curry to “test the waters” and if the development of the site was proving to be successful, MTV planned to take over the site themselves. He claimed to be exploited. MTV, on the other hand, argued that Curry used the registered MTV trademark. It seems like MTV, back in 1993, failed to appreciate the commercial value and potential of a music website and therefore granted all the right to Curry. The dispute was settled quietly on March 24, 1995, and MTV obtained the “mtv.com” domain name.¹⁰⁷

6.16 Roadrunner v. NSI

This is a case that may affect the way domain names are to be registered and challenged in the future. It therefore could be of importance to trademark and domain name holders in the U.S. and perhaps in other countries as well. An ISP in New Mexico called Roadrunner Computer Systems, Inc. (RCS) with over 700 paying subscribers provides computer hardware as well as technical support in order to allow individuals and small businesses to access the Internet. During the spring of 1994, RCS was granted the domain name “roadrunner.com” by NSI. At this point in time, NSI provided domain names solely on a first-come, first served basis. Shortly after, in July and November of 1995, NSI instituted new policies relating to the registration of

¹⁰⁶ *MTV Networks v. Curry*, 867 F.Supp. 1028 (C.D.Cal.1994)
[Http://www.law.seattleu.edu/chonm/Cases/mtv.html](http://www.law.seattleu.edu/chonm/Cases/mtv.html) (971026)

¹⁰⁷ *Trademarks Along the Infobahn: A First look at the Emerging Law of Cybermarks*, by Dan L. Burk, April 10, 1995. [Http://www.nlv-bnc.ca/ifla/documents/infopool/copyright/burd1.htm](http://www.nlv-bnc.ca/ifla/documents/infopool/copyright/burd1.htm) (970725)

domain names. These policies included new rules under which a party holding a registered trademark in any country could lodge a challenge against an existing domain name registration. The trademark should be identical to the domain name in order to challenge it.

The owner of the registered trademark, Warner Brothers, challenged the award of the domain name to RCS claiming that it had a federal trademark registration for the mark "Roadrunner". RCS argued that it had been using the domain name for over a year before Warner Brothers was granted the trademark registration. In its communications with NSI, Warner Brothers did not allege any wrongdoing on the part of RCS.

NSI decided to apply the new domain name policy to all domain names including those which, like "roadrunner.com", were registered prior to the new policy. As a result of the Warner Brothers challenge, NSI required RCS to present a trademark registration for the mark "Roadrunner" within thirty days. In December 1995, Jane M. Hill, president of RCS responded to NSI stating that the words were not identical. The Warner Brothers trademark "Road runner" consisted of two words, not one word as in the case of RCS's domain name. Ms Hill also stated that the two names were used in totally different businesses, and therefore could co-exist. Warner Brothers used the trademark in connection with toys such as dolls, Halloween costumes and masks. RCS provided Internet access services, as explained above. If the domain name would be put "on hold", all the subscribers would be without e-mail and other services. Basically, RCS would be without business. NSI replied that such circumstances were totally irrelevant under the new NSI policy.

The options for RCS was either to give up the domain name to Warner Brothers, present a trademark registration document to NSI within thirty days, or have the domain placed "on hold," to be used by no one, until the dispute between the RCS and Warner Brothers was resolved by agreement, court order or arbitration. RCS obtained several extensions of time from Warner Brothers and NSI. During the extended time (in March 1996) RCS managed to obtain a Tunisian trademark registration for "roadrunner.com". In Tunisia, trademark registrations are granted quickly, often within one or two days. Even though the registration document was sent to NSI within the extended time period, NSI refused to accept it, due to the fact that it was not provided to NSI within the original thirty days after receiving the first notice from NSI, as the new NSI policy required.

6.16.1 Hostile takeovers of domain names

This case raises several interesting questions. According to the NSI policy, a person (A) who finds a valuable registered (with the old policy) domain name used by someone else (B) on the net, could basically register the same word as a trademark. A could then challenge NSI. If B does not have enough money to obtain a foreign trademark or have a court decide it, the domain

name will be put on hold, and eventually A may be able to seize the domain name. Registering the word used in the domain name as a trademark before anyone else does it, could save time and money. It is interesting that NSI did not consider the fact that the two names were used in completely different kinds of businesses. A case like this suggests that domain names and trademarks could infringe upon each other. This does not support the idea that domain names would merely be like street addresses.

Unfortunately for the legal development, the case was dismissed by the court on June 21, 1996. The court held that the original dispute no longer existed between the parties since Warner Brothers agreed to obtain another domain name, "Road_Runner.com".¹⁰⁸

6.17 Summary

The SLD of domain names is a very controversial issue, since only one registration of a name is possible together with the same TLD. Basically, there can exist an unlimited number of different SLDs in each TLD, but there can only exist one specific SLD in each TLD. Most companies around the world crave to have their trademarks registered as domain names, but are often hindered by Cybersquatters or other companies that already registered the desired SLD. I succumb to the opinion of WIPO, that the creation of a universal domain directory service could make domain names which are "easy to remember" less attractive. Companies could use SLDs that do not necessarily reflect the companies' trademarks, since the directory would lead anyone to the right address anyway. If a company finds that a cybersquatter registered its trademark as a domain name, it may be a good idea to fight a legal battle in order to "retrieve" it. If not fought, a cybersquatter could make the name well known in connection with the cybersquatter's business. There is a risk that the cybersquatter will be allowed to use the name in the future and that the name becomes diluted. There are cases as well as facts suggesting that trademarks and domain names are very alike, and could infringe upon each other. I do believe that this is the case, but is not absolutely certain yet. However, I am certain that either laws or cases will clarify the situation concerning trademarks and domain names within a near future.

¹⁰⁸ INTA (International Trademark Association) "White Paper" - *The Intersection of Trademarks and Domain Names*, Feb 5, 1997, Version 1.0. page 12. [Http://plaz.interport.net/int/wpwhole.htm](http://plaz.interport.net/int/wpwhole.htm) (971121)

7 Intellectual Property piracy in Cyberspace

Since the day information became digitized, the possibilities of reproducing such material have undergone a sensational improvement. Because everything posted in Cyberspace is digitized, virtually everything can technically be exactly reproduced without any loss of quality or data. This of course, has lead not only to enhanced lawful reproduction, but also illegal copying of protected material. Suppose a computer program which costs millions of dollars to develop is publicly released Monday. A website owner obtains it, copies it to his website or BBS, and later the same week, the program is not worth more than a freeware. Numerous users will copy (download) the posted software from the web, instead of buying it.¹⁰⁹ Even if the website owner does not post the registration number needed in order to run the program, it is not a problem for the downloaders. Most serialnumbers needed in order to start a program are placed at various sites in Cyberspace. Anyone in need of a registration number in order to start up a pirate copy of a program can find lists containing thousands of numbers.¹¹⁰ Once posted, any material may be reproduced and spread throughout the Internet community, lawfully or not. The incentive to develop new products will certainly decrease if web-piracy is totally uncontrolled. If there does not exist any proper protection for material posted on the web, companies may due to the risk of being exploited, choose not to post any such material out there, and such a move could slow down and possibly harm the development of the electronic commerce. Since it is technically possible to copy almost any digitized material, it is of highest importance that the laws protecting information are effective and enforceable.

7.1 Responsibility for posting, storing and downloading protected material

Who should be responsible for what in Cyberspace? It is obvious that the process of spreading material in Cyberspace involves several different steps. Firstly, there may be a person or company copying protected material from the original source (for example a CD-ROM) without any contact with Cyberspace (at this stage). Secondly, there may be a person or company (possibly the same person or company that created the copy from the

¹⁰⁹ *Deputizing the ISPs – Internet Service Providers should take responsibility for policing copyright infringement in Cyberspace*, by William J. Cook. Intellectual Property Magazine, spring '96. [Http://www.ipmag.com/acook.htm](http://www.ipmag.com/acook.htm) (970716)

¹¹⁰ Serialnumbers to shareware programs are also widely spread in the Internet community. If one searches for “serials” in any search engine, one will find huge lists of numbers to both shareware and complete programs.

original source) posting material to his or someone else's website or Bulletin Board System (BBS), which is a physical place of storage on a server somewhere on the globe. Thirdly, there usually is a person or company (often the ISP) owning and controlling the server where the material is physically stored. The ISP may consent to uploading and downloading protected material. Fourthly, there may be a person or company that, after finding the material located on the server, downloads it into a personal harddrive. Finally, once the material is downloaded, it can be reproduced an infinite number of times, with or without the aid of Internet. This scenario is an everyday matter all over the Internet community. Are all these actions considered illegal? Can all these actions lead to responsibility?

7.2 The first copy made from the original source outside Cyberspace

When a person makes a copy to the harddrive from the original source (such as software from a CD-ROM, a song from a CD, or equivalent) it is not considered an Internet issue since it does not involve Internet at all. It would most likely be considered as a traditional copyright infringement, or equivalent, depending on what material and amount that was reproduced. One must not forget that under certain circumstances, it may be legal to perform a backup copy for personal private use.¹¹¹ (In the U.S. such actions may be legal this is considered to constitute fair use according to the fair use doctrine.¹¹²) Only the closest friends and relatives may use the copy, if it is to be classified as a personal copy. If that is the case, no crime has occurred at this stage. Since not all kinds of material may be copied for private use, one must be careful. I have chosen to further examine the legal situation concerning software, music and pictures.

7.2.1 Copying software off-line

It is not legal to make a personal copy,¹¹³ other than a backup copy, intended for complementary use in case the original copy is destroyed, or if needed for running the program properly.¹¹⁴ It is an interesting fact that, it is illegal to make a personal copy of software in Sweden, while since 1994 there do not exist any legal repercussions relating to such an act.¹¹⁵ Sweden adapted to the *Council Directive of May 1991 on the legal protection of computer*

¹¹¹ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §12:1. The right to make a personal copy cannot be limited by a note attached to the material, saying it is forbidden to make a personal copy. It is, however, possible to limit this right by a mutual agreement. *Lärobok I Immaterialrätt*, by Koktvedgaard and Levin, page 152.

¹¹² *Praktisk IT-rätt*, by Agne Lindberg and Daniel Westman, page 91.

¹¹³ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §12:2.

¹¹⁴ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §26g and §26h. *Nätjuridik – Lag och rätt på Internet*, by Carlén-Wendels, page 76.

¹¹⁵ *Praktisk IT-rätt*, by Agne Lindberg and Daniel Westman, page 91

programs (91/250/EEC).¹¹⁶ Article 7.1 states that appropriate remedies in accordance with national legislation shall be provided by the Member States. Sweden interpreted the directive as not requiring penalization when copying software for private use.¹¹⁷ Therefore, Sweden decided that copying for private use is forbidden and considered illegal copyright infringement, but without punishment.¹¹⁸ This is, however, not the case in all situations. There will be punishment, if the software is used in a business or public activity. The copy may not be used beyond the scope of private use.¹¹⁹ One should keep in mind that other sanctions, such as penalty¹²⁰ of a fine or damages¹²¹ may be appropriate.¹²²

7.2.2 Copying music off-line

A very common feature of Cyberspace is the supply of various music files. Imagine a person buying a record and copies the music into his personal computer or makes a perfect digitized copy with a CD-writer. Since this can be made an infinite number of times, copying for private use is given a completely new dimension. Currently, copying music for private use is allowed in the majority of the EC Member States.¹²³ The major reason for this exception from the exclusive right of reproduction is that the Community does not wish to invade the privacy of individuals. The reproduction must be made for private use and for non-commercial ends. The term “private use” must be understood in a narrow sense, according to the proposal. Eleven out of fifteen Member States compensate rightholders for eliminating their exclusive right with a right to remuneration. It works as a levy system when selling audiotapes. The money collected from the levies goes to the rightholders. For instance, 120 million ECU were collected in France in 1995, as remuneration for private copying.¹²⁴ Interesting is that only one Member State (Denmark) makes a distinction between analogue and digital technology concerning private copying. Denmark, thus, does not provide a private copy exemption regarding material incorporated in digital media. In Sweden, music is protected by law,¹²⁵ and it is considered legal to

¹¹⁶ [Http://www2.echo.lu./legal/en/ipr/software/software.html](http://www2.echo.lu./legal/en/ipr/software/software.html) (971201).

¹¹⁷ Prop. 1993/94:122 page 60.

¹¹⁸ Prop 1992/93:48 page 131.

¹¹⁹ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §53:2.

¹²⁰ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §53a.

¹²¹ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §54.

¹²² *Praktisk IT-rätt*, by Agne Lindberg and Daniel Westman, page 99.

¹²³ Article 5 (2) b in the *Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society*, Brussels, 10.12.1997. COM(97)628 final, page 7.

¹²⁴ *Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society*, Brussels, 10.12.1997. COM(97)628 final, page 18.

¹²⁵ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §2 point 3.

produce a private copy¹²⁶ as long as this is done by the user himself. If another person than the user copies the music, it is considered copyright infringement.¹²⁷

7.2.3 Copying pictures off-line

Pictures are treated similar to other protected material. Photographs enjoy protection independent of quality and originality. In recent years, the majority of the EC Member States have an exception to the reproduction right for photo/print type reproductions (called “reprography”)¹²⁸ combined with a levy system, quite similar to that of audio-visual material. In Sweden it is acceptable to reproduce a few copies for personal use only. The rules are less stringent when it comes to who actually carries out the personal copying. The user may have someone else copying his personal copies for him.

7.3 Legal responsibility when posting protected material in Cyberspace

Before any downloading from the net may occur, material must be uploaded, or posted on a remote server somewhere. Is uploading equivalent of copying? Is it considered illegal to post protected material in Cyberspace? What is the responsibility of the person uploading such material?

7.3.1 Uploading software

Imagine a person owning a legal copy of a software program. This person has a peculiar craving urge to share this software with the rest of the world, by posting a full version of it on a website or BBS server. What kind of legal responsibility would such an action activate? It is, as described above, illegal to copy protected software. Would uploading software constitute a private copy? The result of uploading software to a remote server is that an exact copy of the software is placed in Cyberspace. The original is not sent away from the person uploading it, and therefore it is a matter of copying. A traditional copy is made.

7.3.1.1 Uploading is not equivalent of private copying

By placing the software in Cyberspace, virtually all users in the universal Internet community would gain access to it. In Sweden, this would constitute copyright infringement under the Lag (1960:729) om upphovsrätt

¹²⁶ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §46:2 and §12.

¹²⁷ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §12:3 point 1. *Lärobok I Immaterialrätt*, by Kocktvedgaard and Levin, page 152.

¹²⁸ Article 5 (2) (b) of the *Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society*, Brussels, 10.12.1997. COM(97)628 final, page 18.

till litterära och konstnärliga verk¹²⁹, unless the author gives his consent to the uploading. It is, as described above, not permitted to copy software, even for private use. Even if it *would* be legal to make a copy for private use, I believe it is impossible to consider such an uploaded copy being a private one in most cases. Perhaps if the site where the software is placed is a non-access site secured from other users as well as the ISP by a personal code, it could be considered a private copy. This is irrelevant concerning the lawfulness, since private copying is forbidden but it may be relevant concerning the punishment. As described above, private copying of software does not lead to punishment in some cases.¹³⁰ I am of the opinion that not all on-line copies necessarily must be considered public.

7.3.1.2 On-line backup copy

The on-line copy cannot normally be considered a backup copy either, for obvious reasons. It would therefore constitute an illegal copy.¹³¹ However, if the site is a non-access site, perhaps it could be a backup copy. Imagine a person with very little free harddrive space, who needs a backup copy for his lawfully bought program. If he has a personal place on a server, which *only* he can access, I believe he can use this space for storing his backup copy.

7.3.1.3 The uploading person is responsible

The person uploading software would most likely be held responsible for such an act.¹³² Swedish rules are quite stringent when it comes to posting material on servers. It is not necessary to prove that any downloading has occurred in order to show that illegal spreading of software is at hand. Anyone placing protected software on a host server is by that action alone infringing the copyright.¹³³

7.3.2 Uploading pictures

I am of the opinion, that by uploading a picture (or anything else for that matter) to a website or server, the picture is considered to be spread and redistributed to the public. It is therefore, as with software, not a question of private personal copying. When uploading a protected picture, a copy is transferred to the target site, and this is not allowed unless the author gives his/her permission.¹³⁴

¹²⁹ §12:2

¹³⁰ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §53:2.

¹³¹ This view is supported by the Swedish Högsta Domstolen (HD) in NJA 1996:79 page 90.

¹³² *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 77. The law Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §51:1 says that the person performing the infringing acts, is the one responsible.

¹³³ *Praktisk IT-rätt*, by Lindberg and Westman, page 88

¹³⁴ *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 71.

7.3.3 Uploading music

It is perfectly possible to compress a complete song from a CD to a compression format called MPEG-1 Layer 3 (MP3) without losing any quality. This, due to the fact that music files from a CD are digitized and stay the same (master quality) even though they are compressed and transferred to a harddrive on a computer. A user with a CD-grabber (a program that allows the user to copy songs from CDs to the harddrive) or other ordinary software that comes with CD-writers, can smoothly read the digitized song to the harddrive. Most often, the songs are transformed from the CD standard format CD-DA (Compact Disc-Digital Audio) to the DOS standard format called wave (sometimes referred to as –wav since this is the ending used in Windows). The situation when copying the song to the harddrive in the wave format is not much different from making an ordinary personal copy for private use, as described above. It is a question of copying and reproducing protected material. The only difference is that the copy of the song is placed on the harddrive, and not on some other medium. The wave format is very inconvenient, since songs in this format are extremely memory consuming. A two-minute song will roughly use twenty MB of the harddrive. Therefore, many users choose to decompress the audio-files to MP3 format in order to make storing and electronic transfer more convenient, faster and cheaper. One should keep in mind that there is no notable change in quality. The copy is as good as the original.¹³⁵

Compressing ordinary CD songs can easily be made by using a small program called Layer 3 encoder/decoder (There certainly exists other programs as well) which can be found on the Internet as a normal zipped file ready for extraction.¹³⁶ When entering the Layer 3 directory (in DOS) the user writes for example: “l3enc c:\songname.wav c:\songname.mp3 –hq –br 128000”. This will encode the wave sound-file to a compressed MP3 file. This process is not very fast, and a slow computer could work for hours with a three-minute song. Faster computers can encode several songs at the same time. Once the song is compressed into MP3 format, there exist two copies of the song on the harddrive: one wave file and one MP3 file. Users delete the wave file and keep the MP3 file, which requires much less space on the harddrive. A two-minute MP3 song will approximately use two MB. The MP3 format facilitates the process of sending songs electronically, since the transfer time is reduced enormously.

The MP3 files can be played on the computer’s sound-system using specially designed programs, such as “Winplay” or “Winamp” that can be downloaded from the Internet. Unless the computer is a Pentium with plenty

¹³⁵ The copy will be of master quality if decompressed with a bitrate of at least 128000. A lower bitrate will result in inferior quality.

¹³⁶ Often files are zipped in order to decrease the size of the programs. This is, however, not always the case.

of RAM, playing of such files in the computer sound system will not be of optimum CD-quality. Both Microsoft and Netscape have announced new browsers, which include MP3 players. This will further ease the playing of such files among ordinary Internet users. It is of importance to know that MP3 files cannot be played in normal CD players yet. I believe it may be possible to do so in the future, since there already exist various prototypes of such CD players. However, it is perfectly possible to decode a MP3 song to a normal wave file and write it on a normal CD-R¹³⁷. This procedure is very fast and convenient. A two-minute MP3 song is decoded within seconds in a fast computer. Once the wave files are written on the CD-R, the songs can be played on any standard stereo with perfect master quality. Therefore, anyone with a CD writer and an Internet connection can produce own music CDs without buying traditional music CDs.

7.3.3.1 Uploading MP3 files to a website

Would uploading a MP3¹³⁸ file to a public Internet website constitute copyright infringement? Without the consent and permission of the author, it would¹³⁹ due to the fact that it is not a matter of private use.¹⁴⁰ The copied file is exposed to the public the very same moment it is placed on the website. An undefined group of users can access the copy, and that would be equivalent of spreading the material to the public.¹⁴¹ A European example illustrating this is the French case where Francois-Xavier Bergot uploaded twenty songs by Michel Sardou to his website. The Tribunal De Grande Instance in Paris found this manner unlawful. Bergot contended that the songs were intended for private use. The Tribunal stated that, due to the fact that third parties could access and copy the uploaded songs, the site functioned as an encouragement to use the reproductions.¹⁴²

7.3.3.2 Background music on websites

Sometimes the website owner chooses to play a “background music” to users while visiting the site. The user cannot always decide whether or not to activate the music. If the user’s computer is not equipped with a soundcard and browser with help-applications he/she will not be able to hear the soundfile played. (Sometimes midi-files are used, but more and more often other types of files that can reproduce the music not very much different from the original are used). Today most standard computers as well as webbrowsers are capable of playing such files. Would this “public

¹³⁷ CD-R is a recordable CD.

¹³⁸ MP3 is only a format, but when I use the term I presume that the MP3s consist of protected music songs.

¹³⁹ *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 70.

¹⁴⁰ *Ibid.* page 82.

¹⁴¹ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk §46:1. *Lärobok I Immaterialrätt*, by Kocktvedgaard and Levin, page 134.

¹⁴² *Art Music France v. L’Ecole Nationale Supérieure Des Telecommunications*, Tribunal de Grande Instance Paris [1997]EEC97.

performance” constitute copyright infringement? It depends on the nature of the site. If the music is not the essential part of the site, and the “performance” is non-commercial it is legitimate. Thus, a private website owner would normally not need permission from the author to *play* the soundfiles on the website. However, if the website is a commercial one, permission is required. According to Carlén-Wendels, the difference between non-commercial and commercial sites is merely theoretical, since permission is needed in both situations in order to *place* the copied music file on the site. The “playing” described above is a completely different issue.¹⁴³

7.4 The legal responsibilities of ISPs and BBS operators

Is it possible that ISPs (sometimes referred to as on-line service providers, OSPs) and BBS operators have a legal responsibility regarding uploaded protected material? Are ISPs responsible not only for their own acts, but also for the acts of their subscribers? In the U.S., the Software Publishers Association (SPA)¹⁴⁴ aggressively argues that ISPs are liable under a theory of contributory copyright infringement.¹⁴⁵ Some argue that an ISP is in a situation similar to that of a telephone company supplying the necessary infrastructure. A telecommunications company supplying the physical infrastructure such as wires would not be liable to contributory infringement as a result of subscribers using the phone when committing a crime.

Some argue that ISPs are similar to newspaper publishers. When a newspaper publishes illegal material, the publisher and not the author bears the main responsibility.¹⁴⁶ If one applies the “newspaper model” to the situation of the ISPs, it can be suggested that the ISPs should bear the final responsibility for anything posted by its subscribers. However, one must not ignore the fact that newspaper publishers have a much easier task monitoring published material, than an ISP.

7.4.1 The monitoring of posted information

It may be difficult for an ISP to monitor every single bit of information flowing through its system, since uploading and downloading of diverse material take place rapidly all the time from various places. There are billions of messages flowing across Cyberspace every day. Not all of them

¹⁴³ *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 70.

¹⁴⁴ SPA is an international trade association of the desktop software industry representing publishers.

¹⁴⁵ *Intellectual Property*, by Jeffrey R. Kuester and Daniel R. McClure, The National Law Journal, Jan 20, 1997.

[Http://www.ljx.com/internet/0120ispcp.html](http://www.ljx.com/internet/0120ispcp.html) (971006)

¹⁴⁶ *Tryckfrihetsrätt*, by Håkan Strömberg, page 66.

involve copyright infringements, but the monitoring required to find such infringements would be costly, and could perhaps invade on communications privacy. The ISPs would have to permanently scan the system and monitor all communications, in the search for possible infringements. It has been argued that the ISPs may be best equipped of all parties to supervise the flow of information, if these have enough hardware and software in order to determine when improper material is posted.¹⁴⁷ Some companies, such as Intersect Inc., can help the ISPs finding commonly used formats used to deliver audio and video by scanning the net using Audio Video Scan (AVS).¹⁴⁸ The AVS can scan up to eleven million webpages per day.¹⁴⁹ There exist numerous ways of scanning and monitoring Cyberspace, but whether these are effective in reality, I cannot say. It is possible to watermark music files, but whether pirates will be able to remove such marks remains to be seen. It would be easier for ISPs to determine whether files are infringing copyrights, if all files were tagged with information. Technical equipment, however, is not the only solution to the monitoring. Knowledge of the law is just as important in order to decide the nature of the posted information.

In order to decide which messages that are infringing upon copyrights, ISPs would be put in a position where they must be able to decide whether posted material is infringing copyrights or whether it constitutes “fair use”. Since this is not always obvious, it may not be an effortless task for the ISPs. ISPs would, preferably, have to be educated in IP law in order to determine the nature of the posted information within their spheres. In order to avoid liability, ISPs may be eager to close down anyone that transmits material that *may* infringe upon copyrights. Subscribers may therefore be punished without a fair trial. Subscribers may go out of business, or be offended, if they are shut down without reason and cause. ISPs could lose their customers if they are too threatening to them. If the ISPs, on the other hand, are too lenient, subscribers that are real victims of various infringements may leave the service, or even try to sue the ISPs.

7.4.1.1 The most suitable supervisor

On the other hand, one may argue that ISPs are best equipped of all possible supervisors to hinder copyright infringements in Cyberspace, since ISPs have a relatively close relationship with their subscribers. ISPs possess the power to cut off or ban users not complying with laws, guidelines or basic netiquette. This power, I believe is a special one, not belonging to all other institutions. ISPs may set their own policies and guidelines of compliance

¹⁴⁷ *Deputizing the ISPs*, by William J. Cook, Intellectual Property Magazine, Spring '96. [Http://www.ipmag.com/acook.htm](http://www.ipmag.com/acook.htm) (970716)

¹⁴⁸ PR Newswire, June 2, 1997.

¹⁴⁹ *Tracking and Monitoring Music on the Internet*, White Paper, Sept 1997, by Marco Papa, Ph.D. Chief from Intersect Inc. [Http://www.intersectinc.com/technology.hym1](http://www.intersectinc.com/technology.hym1) (971212)

for the paying (or non-paying) subscribers. They have the ability to seriously warn anyone posting improper material in the on-line community, and I believe such a warning may, in many cases, function as a deterrent. Of course, not all infringing subscribers will be terrified by a threat of terminating the Internet subscription, and as a result discontinue whatever infringing activities they are conducting. However, once the ISP shuts off the subscriber, he/she will not be able to go online using that very same ISP. There is always a possibility that the user simply switches to another ISP and continues the infringing activities in Cyberspace until the next ISP does the same.

7.4.1.2 Transferring the responsibility from the ISP to the subscriber

Imagine ISPs being responsible for the acts of its subscribers. At what point would the responsibility for infringing acts be transferred to the subscribers? There must be actions that the ISP could perform in order to avoid liability, such as warnings or refusal to connect the subscriber to the Internet. Would an e-mail warning (or via traditional "snail mail") from an ISP to an alleged infringer be considered enough steps taken in order to prevent further acts of infringements, and thus avoid ISP contributory liability?

If a subscriber breaks the rules over and over again, the ISPs could simply refuse further access to the web. Should ISPs shut off any subscriber that posts material that *may* be infringing on other's protected material? This is sometimes referred to as the "notice and take down"¹⁵⁰ obligation, which may lead to avoidance of ISP liability. Some may argue that such a method could lead to a situation where subscribers would not dare to post information at all, in fear of being shut down. It could be argued that freedom of speech is endangered, if one is shut down from further access to the on-line community, due to a transfer of completely non-infringing material that is falsely labeled illegal or infringing by a doubtful and perhaps uninformed ISP. This could lead to a situation where Internet users avoid sending any material on-line (at least without encryption) or that users turn to the ISP which apply the least stringent policy concerning the "taking down" and shutting off.

Some argue that since ISPs should bear a greater responsibility due to the simple fact that they receive payment for the services they provide. It has also been said that if an ISP actually uses his authority to pre-check uploaded infringing material but declines to remove it, the ISP should be liable.¹⁵¹ There is a danger in a situation where responsibility only burdens

¹⁵⁰ Statement by Roy Neel, president and CEO of the U.S. Telephone Association. *Senate Judiciary mulls on-line copyright infringement*, BNA, Patent, Trademark & Copyright Law Daily, Sept.5, 1997

¹⁵¹ *Skydd för upphovsrätt på Internet*, by Christina Folkesson, page 22.

ISPs that pre-check uploaded files. Why? If an ISP ignores all incoming material, he/she will not be liable. This may lead to a situation where ISPs never checks any uploaded material in order to avoid liability. Users could then upload any file without ISP intervention.

7.4.2 Cyberspace without ISP liability

If ISPs would not be responsible for the acts of their subscribers, and if ISPs could set their own policies, I believe that the rules and guidelines would be kept at a bare minimum. ISPs would have no interest in searching the Internet for infringing material or warn infringing subscribers. It is likely that the ISP with the least stringent rules and cheapest rates would be the most popular ISP among all subscribers.

7.4.2.1 The U.S. ISP exemption

In the U.S., there has been a turbulent debate during the autumn of 1997, as to whether ISPs should be exempted from liability for any copyright infringements by subscribers. The On-Line Liability Limitation Act¹⁵² (HR 2180) was introduced July 17, 1997 and referred to the Judiciary Committee. The ISPs demanded exemption while creators and producers of movies, recorded music and software opposed such an exemption. The act would make ISPs liable only if six criteria were not met. Firstly, the ISP must not have initially *placed* the material on-line. Secondly, the ISP must not have *generated, selected or altered* the material. Thirdly, the ISP must not have *determined the recipients* of the material. Fourthly, the ISP must not *benefit financially* from the infringement. Fifthly, the ISP must not *sponsor, endorse or advertise* the material. Sixthly, the ISP must not be *aware* of the infringing nature of the material, nor that access to the material is prohibited by law. At a Senate hearing September 4, 1997, the Judiciary Committee was warned that an ISP exemption would allow ISPs to completely ignore online piracy and this could lead to increased piracy.¹⁵³ It has been argued that the cost of piracy in the U.S. is approximately \$18-20 billion a year and that companies depending upon copyrights employ about five percent of the U.S. workforce. One must, however, keep in mind that any figure like that may not be accurate. I am of the opinion that the slogan "Every sale of a pirated item is a lost sale of a legitimate item"¹⁵⁴ is not true. Many people who buy or download pirate copies would never have bought the original, due to lack of financial strength. If these people get their hands upon a cheap or free pirated version, they obtain it, but if they would have to pay full price they do not.

¹⁵² BNA's Electronic Information Policy and Law Report, July 18, 1997, page 741 and 778.

¹⁵³ *Internet Service Providers seek to be shielded from laws targeting pirates*, by Bob Dart. The Atlanta Journal, Sept. 5, 1997, page 11A.

¹⁵⁴ Electronic Engineering Times, August 11, 1997, by Brian Rost, page 115.

7.4.3 European proposals concerning ISP liability

A proposal for a Directive harmonizing aspects of rules on copyright and related rights in the Information Society has been presented to the European Commission¹⁵⁵. However, the proposed Directive does not include provisions concerning liability of ISPs, due to the fact that liability is a horizontal issue. Liability of ISPs is to be included in a specific proposal for legislation that will be put forward by the Commission during 1998.¹⁵⁶

In Sweden, a new law has been proposed to ensure that BBS-operators have a legal responsibility to eliminate any posted information that in an obviously way infringes upon protected material.¹⁵⁷ The proposal states that BBS-operators will have a right to read and control all material flowing through the system in order to detect and remove infringing material.¹⁵⁸ The BBS-operators, however, will not be liable for the infringing material, but they will be liable for not removing such material.

7.4.4 Cases suggesting that ISPs or BBS operators have a legal responsibility

Several cases suggest that operators of electronic bulletin boards (BBS) allowing users to upload and download copyrighted material are liable to copyright infringement.

7.4.4.1 NJA 1996:74

This is a Swedish case where a Swedish BBS operator, Fredrik H, made over 1000 protected software available to the public on his BBS. At least 300 paying users could access and download the protected software from the BBS using a modem and a computer. Users could upload, trade and download whatever software they desired after they had paid a base fee to Fredrik. He, himself, merely stored the uploaded software in his base, and under such circumstances, it could not be said that Fredrik produced copies of the software himself. However, it was stated that by allowing 300 persons to barter, borrow and download over 1000 protected programs without the consent of the owners, it was a matter of copyright infringement. Fredrik claimed that the 300 persons in question, all were his close friends, and that the matter therefore was within the private use sphere. The court, however, basically said that nobody has 300 close friends, and ignored Fredrik's claim. Therefore, the BBS operator was responsible for allowing users (not being family or close friends) to access the protected files.

¹⁵⁵ Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society, COM(97)628. Dated Brussels. 10.12.1997.

¹⁵⁶ Single Market News, The Newsletter of DG XV – Internal Market and Financial Services, No 10, Dec 1997, page 22-23.

¹⁵⁷ 5 § Lag (1998:000) om ansvar för elektroniska anslagstavlor.

¹⁵⁸ Prop. 1997/98:15 page 4.

7.4.4.2 Playboy Enterprises v. Frena¹⁵⁹

A BBS operator, George Frena, could not escape liability for copyright infringement, although he was not aware that his subscribers uploaded and downloaded over 170 copyrighted Playboy photographs from his BBS.

Frena claimed that he never uploaded any of Playboy's photographs onto his BBS himself and that only subscribers to his BBS uploaded photographs. Frena further stated that he himself had never placed the pictures, nor the words "Playboy" or "Playmate" onto the BBS. Frena said he innocently and without malice, allowed subscribers to upload whatever they wanted onto his BBS. As soon as he was made aware of the matter, he removed the photographs from his BBS. He further claimed that he then monitored the BBS to prevent additional photographs of PEI from being uploaded. An interesting fact is that Frena attempted to take credit for Playboy's work by placing its own advertisement with its phone number on some of the photographs. Such removal of Playboy's trademarks from the photographs constituted "reverse passing off" according to the court.

Public distribution of a copyrighted work is a right reserved to the copyright owner. The court concluded that the display on the BBS of Playboy's copyrighted photographs to the subscribers was a matter of public display. It was therefore, a matter of infringement. I find it interesting that Frena was found liable for infringement, even though he may have been unaware of the files being copied. The court stated: "It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement".¹⁶⁰ This states that BBS operators and perhaps ISPs can be liable even though they are not aware of the infringing. Lack of knowledge may therefore not a valid defense. It gives an incentive to scan and monitor every message flowing through a system, in order to avoid liability.

7.4.4.3 Sega Enterprises Ltd. V. Maphia¹⁶¹

Sega, the video game manufacturer filed a suit for copyright infringement against a BBS called Maphia. Chad Sherman (Sherman) was the system operator of the BBS Maphia, which had about 400 users swapping files. Users needed a password in order to log on to the BBS.

Sega received an anonymous tip that Sherman operated a BBS, which contained and distributed pirated and unauthorized versions of Sega's video

¹⁵⁹ *Playboy Enterprises, Inc. v Frena*, 839 F. Supp. 1552 (M.D. Florida 1993)

[Http://www.leefrog.com/E-Law/Cases/Playboy_v_Frena.html](http://www.leefrog.com/E-Law/Cases/Playboy_v_Frena.html) (971212)

¹⁶⁰ Quoting the court.

¹⁶¹

[Http://www.leefrog.com/E-Law/Cases/Sega_v_MAPHIA2.html](http://www.leefrog.com/E-Law/Cases/Sega_v_MAPHIA2.html) (971208)

game software. At the time of the raid, the Maphia BBS contained twelve unauthorized copies of Sega games, ten Sega-licensed games, and six Sega beta version games. It was proved in the case that Sherman was well aware of the fact that the users uploaded and downloaded copyrighted games from the BBS.

Sega stated that Sherman, as the BBS operator, was liable for copyright infringement. In order to have Sherman liable of direct copyright infringement, Sega had to prove its ownership of a valid copyright in the infringed work, and that Sherman had copied the material. Sega could not prove that Sherman did the copying himself. However, nobody could deny that copies were made, as the files were uploaded and downloaded from the Maphia BBS, and thus, copying made by *someone* was a fact. Since Sega could not prove that Sherman directly caused the copying, he could not be liable for direct infringement.

Sega then claimed that Sherman was liable for contributory infringement. Contributory copyright infringement stems from the idea that one who directly contributes to another's infringement should be held liable. In order to prove that, Sega had to establish that the users of the BBS directly infringed Sega's copyright. Sega also had to establish that Sherman knew about the infringing activities, and that Sherman materially contributed to, caused or induced the infringing activities. Sega managed to prove all of the above. Sherman had intentionally contributed to the users' infringement of Sega's copyright.

Sherman argued that the copying of files fitted under the fair use defense since the users solely used the copies at home and that any copyright violation was de minimis. The court found that Sherman failed to prove fair use, and thus stated that Sherman's role in the copying of Sega games was a case of contributory copyright infringement.

7.4.5 Cases denying ISP or BBS operator responsibility

7.4.5.1 NJA 1996:79 "The BBS-case"

This is a Swedish case from 1996, where a Swedish BBS operator, Lars R, allowed subscribers to upload and download various software. At least 35 copyrighted programs were found on the BBS. About 40 users were allowed to download all files (including the copyrighted ones), while other users had access only to other programs (most shareware, freeware and beta-versions). The Swedish Supreme court, Högsta Domstolen (HD) held that in general, uploading as well as downloading of protected software is copyright infringement, since it is not a matter of private use. This was, however, not

the main question in the case. The basic question was, if solely placing a BBS at disposal is enough to fulfill the requirement of activity needed in order to establish that copyright infringement has taken place. The court stated that the requirement of activity was not fulfilled due to the fact that Lars R had not done anything to the files placed in his BBS. He was passively watching the users uploading and downloading the software. If Lars R had tried to destroy the files or limit the access to them but failed partially to do so, the requirement of activity would have been fulfilled and he would have been liable for copyright infringement. The message of the court is basically the following: do not try to remove protected software from the BBS unless you are 100% sure that you will be able remove all files. It is better not to care in order to avoid fulfilling the requirement of activity. The court declared that the law¹⁶² was not prepared for modern problems like this, and needs to be revised in order to offer a satisfactory protection for software when stored on a BBS.

7.4.5.2 Zeran v. America Online¹⁶³

Kenneth M. Zeran (Zeran) was a victim of a distasteful hoax perpetrated via the Internet services of America Online, Inc. (AOL). Somebody posted Zeran's name and phone number together with an advertisement for t-shirts and other items carrying various slogans glorifying the Oklahoma bombing in which 168 people died. Of course, Zeran was bombarded with disturbing and threatening telephone calls from people who were offended by the posted notice. Zeran complained to AOL (Zeran was not an AOL subscriber) and asked to have the disgraceful messages removed. The same day (April 26, 1995) as these were deleted, another similar message was posted. Zeran had to put up with more angry phonecalls. The person or persons posting the messages could not be found since false names had been used when registering the AOL service. On May 1, 1995, a radio station in Oklahoma read the posted notice on the air and encouraged listeners to call Zeran and tell him how disgusted they were. Zeran received numerous death threats from angry people believing that he vendited the offending material.

Zeran sued AOL and claimed that AOL had been negligent due to the fact that AOL allowed the notices to remain and reappear on AOL's BBS even though Zeran had noticed and complained about it. Zeran claimed that distributors of information are liable for distributing material which they know is of a defamatory character. AOL required the case to be dismissed since it violated section 230 of the Communications Decency Act of 1996 (CDA). AOL argued that by imposing liability on it for harm caused by the posted messages, it would be treated as the "publisher" of third-party content. This would require supervising, editing and censoring of all material originating from third parties. Zeran claimed that section 230 would

¹⁶² Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk

¹⁶³ *Zeran v. America Online*, 958 F Supp.1124 (E.D. Va. 1997)

[Http://www.bna.com/e-law/cases/zeran.html](http://www.bna.com/e-law/cases/zeran.html) (971208)

not hinder his suit, due to the fact that he did not seek to impose liability for “publishing” the messages. He sought to impose liability on AOL for “negligently distributing” the posted messages after being informed that these were bogus ads. The court stated that Zeran’s suit was in violation of section 230. AOL was not found to be responsible for the posted messages on the BBS.

7.4.5.3 Doe v. America Online Inc.¹⁶⁴

In 1994, Richard Lee Russell (Russel) committed sexual battery on John Doe (Doe), who was then eleven years old, and two other minor males. The small boys were forced to perform various sexual activities with Russel and with one another. These sexual acts were videotaped and photographed. Russel used AOL services such as AOL chat-rooms in order to sell the videotape and the photographs to other subscribers. Doe stated that AOL had been informed that its service was being used for marketing of child pornography material. Doe had also complained to AOL regarding Russell.

Doe sued AOL claiming that AOL had been negligent and violated Florida criminal obscenity laws since it had not earlier prevented Russel’s activities on its services. The reasoning of the court was very similar to that in *Zeran v. AOL*, since the court based its decision upon it. Doe’s claims were dismissed. AOL was not responsible for the detestable acts of Russel.

7.4.6 Music archives in Cyberspace

During the end of 1996 and the beginning of 1997, websites started to supply the Internet community with huge archives of songs in MP3 format. Anyone visiting such a website or FTP can often find very new and popular songs, ready for downloading. The website owner usually never charges anything. It is a peculiar situation, since we all know that “there are no free lunches”. Sometimes, however, users are encouraged to upload songs to the sites.¹⁶⁵ Why would anyone take the risk of supplying the Internet community with illegally uploaded songs, without any financial gain at all? Perhaps websites that generate a high number of hits are able to receive profitable contracts with unscrupulous advertisers, not afraid of being

¹⁶⁴ *Doe v. America Online Inc.*, CL 97-63(Fla. Cir. Ct., Palm Beach Co.1997
[Http://www.navitus.com/icons/networklaw/case_Doe.htm](http://www.navitus.com/icons/networklaw/case_Doe.htm) (971208)

¹⁶⁵ Some sites are “ratio sites” where you are not allowed to download anything if you do not upload new (not already stored in the site) material prior to downloading. For instance, some sites could call themselves 1:5 ratio sites, meaning that if one uploads one MB, one is allowed to download five MB from the site.

associated with pirate websites¹⁶⁶, but I am sure this is not the general situation. The music industry, I believe, did not realize the potential danger of the growing number of music archives in Cyberspace at first. During the late spring and early summer of 1997, the music industry reacted to this extremely rapidly growing hobby of many devoted Internet users throughout the Internet community. It was the British pop group Oasis that partly triggered the contentious debate concerning copyright in Cyberspace. Some pop bands, such as U2 discovered their tracks available on the Internet before officially released.¹⁶⁷

The music industry in the U.S. was terrified, and the Recording Industry of America (RIAA) requested, on behalf of several of its members, the shutdown of three U.S. websites distributing sound recordings on June 9 and 10, 1997. Federal district courts in California, N.Y. and Texas issued temporary restraining orders directing the ISPs to completely block the unauthorized recordings, and to guard the evidence.¹⁶⁸ Three lawsuits were filed against the archive sites¹⁶⁹ and are considered to be first of this kind. The three operators may face up to \$100,000 in damages for each infringed copyrighted recording.¹⁷⁰ The RIAA strives to put current copyright law to the test in the context of the Internet. In the meantime, many companies anxious to protect their copyrights against the increasing problem of digital piracy hire digital detectives that surf the Internet searching for infringements.¹⁷¹

7.5 Legal responsibility when downloading protected material

One must not forget that every day millions of people around the globe download material that they find on the Internet. Much of this material is, of course, protected. Who is liable when downloading of such material occur? Is the situation the same concerning software, music and pictures? Are all users who download protected material from the net, infringing upon somebody else's copyrights?

¹⁶⁶ It seems like the porn-industry does not care if its banner ads are displayed in connection with illegal music archives and other warez sites.

¹⁶⁷ The Guardian (London), May 16, 1997 page 12. One can only speculate how anyone can receive a track not yet released.

¹⁶⁸ BNA Patent, Trademark & Copyright Law Daily, June 13, 1997.

¹⁶⁹ Known as: ftp://208.197.0.28 and ftp://parsoft.com/MP3s and Fresh Kutz. All the operators were not identified at the time of the suits.

¹⁷⁰ Daily Variety, June 10, 1997, page 1, by Christoffer Stern.

¹⁷¹ The Financial Post, August 28, 1997, by Alice Rawsthorn, Financial Times.

7.5.1 Responsibility when downloading software from the Internet

There are various kinds of software that one may encounter in the virtual world. If the software is a so-called “freeware”, it is to be distributed freely. By downloading such a program, no infringing what so ever is at hand. Another kind is the “shareware” which can be downloaded and used freely only for a limited time. If one decides to keep the shareware program, one must pay a specified amount to the author. Often, shareware is equipped with “nag screens” reminding the user of the obligation to pay the fee within time, or “time limits”. In order to remove the nag screens or open up the program after the time limit expired, one must pay the fee in order to receive a code.¹⁷² I have no intentions of further studying neither freeware nor shareware in this thesis. I find it more interesting to consider software not intended for Internet downloading i.e. software that is illegally uploaded in Cyberspace and downloaded by regular users. Imagine a person that for some odd reason wants to achieve a high number of “hits” (a user visiting a site is considered to cause a “hit”) on a particular site. This person may store a copy of attractive protected software on his website. Would it be illegal if another person finds this software on the site and downloads it to his/her own computer in order to use it privately?

In Sweden, as described above, software cannot be copied, even for private use¹⁷³ unless it is a backup copy not to be utilized unless the original is destroyed or lost. It is therefore not legal to copy protected software placed in Cyberspace. The fact that somebody else committed a crime by uploading software in Cyberspace in the first place, is no excuse for downloading it.¹⁷⁴ It is certain, that downloading software is equivalent of producing a copy from one computer to another.

One could argue that downloading software is a matter of copying within the private sphere, which in Sweden, of course, is illegal¹⁷⁵ but without punishment.¹⁷⁶ This may very well be true, but in some cases I believe the Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 53:2 cannot be applied. If a private copy is made from software originating from public businesses, this cannot be excepted from punishment even though the copy is intended for private use only. If such a copy is placed in Cyberspace,

¹⁷² As described above, serial number archives are popular reading in Cyberspace.

¹⁷³ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 12§.

¹⁷⁴ *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 77.

¹⁷⁵ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 12:2.

¹⁷⁶ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 53:2.

the downloading of the copy for private use is (as always) illegal *but* it may be punished since 53:2 is not applicable.

If one downloads a copy from the Internet, it could be argued that the copy (made between the site owner and the downloader) is not made within the private sphere, and therefore is illegal. The person offering the software in Cyberspace does not know the persons downloading it. It is possible that one could maintain that second generation copies made from illegal copies never can be made for private use and be excluded from punishment according to the Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 53:2. Most copies of popular software found in Cyberspace are probably illegal copies according to this reasoning. It is hard to believe that someone places an original copy onto a server. However, it may be difficult to decide whether the software is a copy or an original, since they both are digitized and identical.

It is possible that a copy within the private sphere made from an illegal copy is illegal and that Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 53:2 cannot be applied. If this is the case, all downloading of protected software from the Internet is illegal (even within the private sphere) and can be punished according to Swedish law. Whether a copy of a software can be copied an additional time (from the Internet) and still be covered by 53:2 is not mentioned in the law, nor the preparatory work.¹⁷⁷ Since it does not seem to be totally clear whether illegal software copies can be copied an additional time for private use without being punished, persons downloading such software could possibly claim that they are merely making a copy for private use, and therefore cannot be punished. It could be argued that it does not matter whether the private copy is made from the original or from a copy. I am of the opinion that the situation is unclear, whether one must copy (for private use) from an *original only*, in order to avoid punishment according to the Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 53:2. Is a *copy* of the software (not the original) found in Cyberspace included in the meaning of the law in 53:2?

7.5.2 Responsibility when downloading music from the Internet

Imagine an Internet user, situated in Sweden who discovers a website containing uploaded musicfiles and he/she decides to download a few songs. Is the downloader infringing any copyrights by such an action? In Sweden, it is as described above, legal to copy music for private use, if the music lawfully has been made available to the public.¹⁷⁸ It is, however, required that the downloader does not spread the music outside the private sphere.

¹⁷⁷ Proposition 1992/93:48 Skydd för datorprogram, page 131 and forwards.

¹⁷⁸ Lag (1960:729) om upphovsrätt till litterära verk och konstnärliga verk 81, 12§ and 46§.

One could therefore say that users are allowed to download music from the Internet if the music is for private use only.¹⁷⁹ Thus, if the user only as much as *offers* a copy of the downloaded musicfile to anyone not being family or close friend, it would constitute infringement.¹⁸⁰

I believe that if a user finds music that has not yet been officially released to the public,¹⁸¹ it would constitute an infringement, since such music cannot be copied even for private use.¹⁸² It would, however, not always be obvious to all users whether or not a song has been officially released.

One could argue that users should know that much of the musicfiles found in Cyberspace are uploaded by someone lacking permission from the rightful authors, and that the musicfiles therefore are infringing upon copyrights. It is true but it does not eliminate the right to produce a private copy. In the above-mentioned French case, the Tribunal de Grande Instance in Paris said that there is an implicit authorization to copy when visiting a private webpage.¹⁸³ This may sometimes very well be the case, if there does not exist any disclaimer or written text that explicitly prohibits downloading of any kind.

7.6 Summary

With the age of digitizing, copies and originals have exactly the same quality. One could say that intellectual property piracy is here to stay and flourish. Faster connections will allow very large programs and files to be transferred electronically between users in no time. At this point in time, Cyberspace provides numerous opportunities for persons around the globe to barter and copy material. Everyday and night thousands of programs and files travel through the telecommunication infrastructure. These activities are more widely spread than most software producers can ever imagine.

Copying software for private use in Sweden is not lawful any longer, but there does not exist any punishment for such actions. Uploading software in Cyberspace is equivalent of producing a copy and is therefore illegal. Such a copy cannot constitute a private copy, and therefore may such actions be punished according to Swedish law. Downloading protected software from Cyberspace is illegal. The question of whether such actions (for private use) will be punished in Sweden is, however, unclear if one analyzes the law and the preparatory work.

Nowadays music is being compressed into small handy files that can be transferred from one continent to another within minutes. An interesting fact

¹⁷⁹ *Nätjuridik, Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 70.

¹⁸⁰ *Praktisk IT-rätt*, by Agne Lindberg and Daniel Westman, page 88.

¹⁸¹ Such as the unreleased U2 songs mentioned above.

¹⁸² *Praktisk IT-rätt*, by Agne Lindberg and Daniel Westman, page 109.

¹⁸³ *Art Music France v. L'Ecole Nationale Supérieure Des Telecommunications*, Tribunal de Grande Instance Paris [1997]EEC97.

is that the music can be written on a CD-R and be played in any stereo, with the same quality as the original CD. Uploading a music file to a website or equivalent constitutes copyright infringement absent permission from the author. Downloading such files is lawful within the private use sphere.

The question of ISP and BBS-operator liability is an infected issue in many countries. Sweden has proposed a new law, making the BBS-operators liable for not removing infringing material. There are cases suggesting as well as opposing ISP liability.

8 Jurisdiction

8.1 The importance of jurisdiction in the world of information technology

Jurisdiction is an extremely important issue, because a judgement by a court without proper jurisdiction over a defendant is considered void.

Traditionally jurisdiction required physical presence within the territorial boundaries of the court, but this has gradually changed. In Cyberspace, people from all over the world gather and exchange various kinds of information without even reflecting upon the fact that there exists physical borders between them. It does not matter any longer (technically speaking), where on earth one is located, as long as one has a computer and an Internet connection available. Even though it may look like it, one cannot claim that Cyberspace consists of one national jurisdiction solely, since the network is omnipresent and universal. The users in Cyberspace are situated in separate different countries with different legal frameworks and traditions. Therefore it may be hard to determine which jurisdiction's law that applies. It is not a problem exclusively between miscellaneous countries around the world. It is also a problem relating to the different states within the U.S.

The rapid technological development may result in a situation where companies and individuals are submitted to jurisdiction in a wide range of places all over the world as a result of posting information on a single website. Materials published in Cyberspace may be read, downloaded, and copied by people in various countries around the world. Most of these countries have different laws, and authors must take into consideration that publishing their work on the Internet could expose them to liability in those countries. Even if a web advertiser wishes to aim an advertisement only to a specific location, the technology enables all users on-line around the globe to receive the messages, unless certain unattractive security measures are taken. Does this lead to a possibility to sue anywhere in the world, if not technological barriers are used to hinder omnipresent access to the posted messages? Should courts focus on the *intended* receivers of a specific website, or should they concentrate on every user that has the *possibility* to access the material? What if a web advertisement clearly excludes every jurisdiction except one, by referring to a posted disclaimer stating that the products or services offered are solely available to customers in a specific jurisdiction? Would it be reasonable to sue such an advertiser in another jurisdiction than the targeted one? Some argue that it would be reasonable to sue in a "disclaimed jurisdiction" only if the advertiser is *aware* that he sells products or services to customers situated in a "disclaimed jurisdiction".¹⁸⁴

¹⁸⁴ *Solicitation via the Internet; Jurisdiction over Claims* by Edward Brodsky, The New York Law Journal, June 11, 1997

What exactly does this mean? If the company makes business in a jurisdiction that has been excluded by a disclaimer, as described above, it would be possible to sue the company only if it is proven that the company is aware of the location of its customers. It has been suggested that courts also should take into consideration whether the advertiser uses available technological barriers in order to filter out residents of certain jurisdictions and exclude them from receiving the messages. Some kind of written application from the customer that would identify his jurisdiction is mentioned as an example.¹⁸⁵ The buyer could fax or e-mail to the seller, who sends back, via e-mail, a password and a user name. The customers in certain desired locations would then be accepted and receive access to the information. However, such complicated procedures may discourage some buyers, which may have a negative effect on the trade.

If one wishes to advertise on the Internet, one must bear in mind that a potential plaintiff may in some cases be allowed to choose the most favorable law to him, depending on the claim he wants to pursue.¹⁸⁶ Such forum shopping¹⁸⁷ may complicate the situation. The website owner may have to defend himself in jurisdictions in which he is not a resident. All over the world, jurisdictional issues regarding the Internet are controversial issues. In some places, such as Minnesota for instance, the arrangement used to exercise jurisdiction is considered very arguable and controversial from an international perspective. If countries do not respect each other's methods and strive for harmonization, jurisdictional issues on the Internet will be even harder to resolve in the future.

8.2 Swedish rules concerning jurisdiction

It is important to notice that at this point in time there does not seem to exist any Swedish cases relating to the Internet and jurisdiction. Do Swedish courts have jurisdiction over foreign web-editors posting information not complying with Swedish penal laws, due to the mere fact that the sites can be accessed and viewed in Sweden (and certainly in most other countries as well)? If the posting of information takes place in a foreign jurisdiction, the place of the alleged crime is not Sweden. The place of the crime is the place where the act was completed, i.e. in the jurisdiction where the posting occurred. Therefore, one certainly must find a rule of jurisdiction, which allows Swedish law to be applied. If the web-editor (the person) has a strong connection to Sweden, such as a Swedish citizenship, or domicile, the

([Http://ljextra.com/Internet/061irsolic.htm](http://ljextra.com/Internet/061irsolic.htm)). Mr. Brodsky is a partner at Proskauer Rose LLP.

¹⁸⁵ Ibid.

¹⁸⁶ *Solicitation via the Internet; Jurisdiction over Claims* by Edward Brodsky, The New York Law Journal, June 11, 1997

([Http://ljextra.com/Internet/061irsolic.htm](http://ljextra.com/Internet/061irsolic.htm)).

¹⁸⁷ *Svensk internationell privat- och processrätt*, by Michael Bogdan, page 34.

“active personality-rule”¹⁸⁸ may be applied. Another situation that may allow the application of Swedish law is if the crime is specifically directed towards Sweden, and therefore has a close connection to Sweden.¹⁸⁹ One must also consider whether or not the posting of material is illegal in the jurisdiction in which the posting took place.¹⁹⁰ It may be difficult to have a Swedish ruling executed in another jurisdiction, especially if posting the information is not criminalized there. Concerning damages in civil cases, the forum delicti, i.e. the place of the damage, may be of importance.

The sometimes very complicated issues relating to jurisdiction are facilitated by various conventions, in which states voluntarily agree to accept and execute each other’s rulings etc. When no convention is applicable, Sweden is forced to apply Swedish law only within the Swedish borders.¹⁹¹ It has been suggested that Sweden must limit the applicability of Swedish law only to matters with a close relationship to Sweden and thus accept foreign websites that do not specifically turn to a Swedish audience. If a foreign website is written in the Swedish language, it may be reasonable to apply Swedish law, since the website then is clearly directed towards Sweden and its’ interests.¹⁹² This approach to foreign websites differs very much from that of the American Minnesota approach, described below.

8.3 U.S. jurisdiction issues in brief¹⁹³

State courts can in certain circumstances decide in matters involving nonresidents, who do not consent to be sued in the state, never visited the state, nor opened an office in the state. Federal courts can assert jurisdiction over persons within the territorial borders of the state in which the court is situated. Federal courts may also use long-arm statutes (state jurisdictional laws) over nonresidents, in order to have the same reach as local state courts.

If a person has certain minimum contacts with the forum and the suit does not offend traditional notions of fair play and substantial justice, a court may have jurisdiction over him. The person should, based upon his contacts, be able to foresee and anticipate being haled into court in the jurisdiction. A court may find jurisdiction over a foreign business if it purposefully availed itself of the privilege of conducting activities within the forum state.

¹⁸⁸ Brottsbalken 2:2 p2.

¹⁸⁹ The “passive personality-rule” in Brottsbalken 2:3 p4.

¹⁹⁰ Brottsbalken 2:2:2.

¹⁹¹ *Nätjuridik – Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 33.

¹⁹² *Ibid.* page 34.

¹⁹³ *Cyberlaw – The law of the Internet*, by Jonathan Rosenoer, page 227-230.

Electronic contacts are commonly used today, and may give rise to jurisdiction, if the electronic contacts are purposefully directed and have a significant connection to the litigation.

American cases covering Internet and jurisdiction issues

At this moment, there exists very few cases concerning Cyberspace and jurisdiction, and most of them emanate from the U.S. Being a European, one should not completely ignore the U.S. cases, since Europe is roughly lagging two or three years behind the U.S. concerning the Internet, and any innovative legal solution regarding novel technologies found by U.S. courts, may be of interest even for European countries with different legal systems. The U.S. has sometimes been criticized for its eager to apply its federal laws towards foreigners, even when American interests are not at stake. Even though many of such judgements and sentences are not executable in all countries, they could have a serious affect upon the people or companies in question. This, because the U.S. is such a mighty business nation and people around the world depend upon the U.S. in many situations. One could be arrested if visiting the U.S., or one's property in the U.S. could be confiscated etc.¹⁹⁴

There surely exists other Internet related U.S. cases concerning jurisdiction issues, but I restricted this study to cover the ones I find most relevant and interesting. When analyzing the cases below, one receives the impression that the courts are striving towards a more relaxed attitude concerning the criteria needed in order to establish jurisdiction over out-of-state Internet users. This may be a desperate attempt to gain control over the various activities that take place in Cyberspace, as the technology is developing at such a rapid speed that governments fear that present laws may soon be superfluous. Some of these cases have been criticized for not fully comprehending the new medium in the electronic Cyberspace.¹⁹⁵

¹⁹⁴ *Nätjuridik – Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 33.

¹⁹⁵ *Government in Cyberspace - What Jurisdiction*, NZ Institute of Public Administration (Inc.), Governance in Cyberspace Conference, 17 April 1997, presented by Michael Cronin and Bernadette Jew.
[Http://www.rmmb.co.nz/cybergovhtm](http://www.rmmb.co.nz/cybergovhtm)

9 American cases in which jurisdiction is granted

9.1 United States v. Thomas¹⁹⁶

This is a criminal obscenity case from 1996 where Mr. Robert Alan Thomas and his wife Carleen Thomas operated (from February 1991) a BBS on a computer in their home in Milpitas, California called "Amateur Action," from which subscribers could download pornographic materials. Mr. Thomas converted pictures from adult paperback magazines to Graphic Interchange Format files (GIF) by using a scanner and stored these in the harddrive of his computer. The BBS contained close to 14,000 GIF files. The Thomases also made it possible to order adult videotapes by e-mail and have them delivered by the United Parcel Service (UPS). Surfers who were not members could only view the introductory screens, which contained descriptions of the material posted deeper into the web-system. In order to view all the GIF files, membership was obligatory. After paying a membership fee of \$55 and submitting a signed application form (including the applicant's address), a personal password would be sent, granting full access to the deeper sites of the BBS.

9.1.1 The California website distributed obscene material in Tennessee

As part of an undercover operation in 1993, David Dirmayer, a federal postal worker in Tennessee applied and received full access to the Californian BBS. Mr. Thomas e-mailed and spoke to Mr. Dirmayer on the phone, and therefore knew Mr. Dirmayer was a resident of Tennessee. Mr. Dirmayer downloaded some of the GIF files and ordered six adult videotapes, which were delivered to an address in Tennessee by the UPS.

9.1.2 The obscene downloaded material did leave the Californian website

Mr. Dirmayer brought a criminal complaint against the Thomases for distributing obscene material in Tennessee. The Thomases argued that they had no intention of distributing the material in Tennessee and that the material never left their home since the member himself had pulled the material into a foreign jurisdiction. The court rejected this argument. It is illegal to receive, transport or distribute obscene material and apparently this was the case when posting material on a website. It is unfortunate that the court did not further explain when information on a site is considered to have left the jurisdiction.

¹⁹⁶ *United States v. Thomas* 74 F.3d 701 (6th Cir.). January 29, 1996.

9.1.3 Refusing customers in certain jurisdictions in order to diminish risk of liability

If the Thomases would not have wished to subject themselves to liability in jurisdictions with less tolerant standards for determining obscenity, they could have refused to supply passwords to members in those districts, thus diminishing the risk of liability. The court seemed to find personal jurisdiction merely on the accessibility of the site¹⁹⁷, and the fact that Mr. Thomas had clear intention to avail himself of the Tennessee market, because he requested information about the applicant and thus knew that the applicant was situated in Tennessee. This knowledge did not stop him from providing the necessary password to the applicant. The effects of Mr. Thomas' conduct had reached Tennessee, and therefore Tennessee was considered the proper jurisdiction. As a result of this reasoning, the Thomases were convicted and sentenced to two and a half years in prison.

9.2 Inset Systems, Inc. v. Instruction Set, Inc.

¹⁹⁸

This case from 1996 is considered to be in the gray area between the two extremes, meaning that neither the passive contact standard, nor the active contact standard is met. Inset Systems, Inc. (Inset), a Connecticut corporation brought trademark infringement action against Instruction Set, Inc. (ISI), a Massachusetts corporation which used its trademark "Inset" as the Internet domain name "Inset.com". ISI filed a motion to dismiss for lack of personal jurisdiction. In 1995, when Inset attempted to obtain the above mentioned domain address, Inset found out that it was already taken by ISI. ISI also used the phone number "1-800-US-INSET" when advertising its products on the web. There was no kind of authorization from Inset to use its trademark "Inset" in any way.

9.2.1 Website advertisement fulfilled the "minimum contacts test"

Since March 1995, ISI had been advertising its products on-line, and there were at least 10,000 access sites on the web in Connecticut. The court stressed the power of the Internet as an advertising medium, stating that "...unlike hard-copy advertisements... which are often quickly disposed of and reach a limited number of potential consumers, Internet advertisements are in electronic printed form so that they can be accessed again and again

¹⁹⁷ *Extending Personal Jurisdiction to Acts in Cyberspace*, by Dane Steffenson for Law 7333 (Law & The Internet) spring semester 1997 at Georgia State University College of Law.

¹⁹⁸ *Inset Systems, Inc. v. Instruction Set, Inc.* 937 F.Supp.161 (D. Conn.1996) April 17, 1996. [Http://zeus.bna.com/e-law/cases/inset.html](http://zeus.bna.com/e-law/cases/inset.html) (970925)

by many more potential consumers.”¹⁹⁹ This quality of continuous contacts that Internet provides, fulfills the “minimum contacts test”²⁰⁰ according to the court. By posting the advertisements on the web, ISI had purposefully availed itself of the privilege of doing business with Connecticut and could therefore reasonably anticipate the possibility of being hailed into court in there. ISI had posted an 800 number, which could be seen as an indication that the site was trying to get in contact with residents outside Massachusetts. However, there was hardly any discussion whether the site was ever visited or if the number ever used, or if ISI had any knowledge of Connecticut residents accessing the site or calling the number.²⁰¹

I find this reasoning very peculiar. The only contact was the advertisement with the 800 number on the webpage, but still the court stated that ISI had purposefully availed itself to the benefits of the privilege of doing business in Connecticut. Are web operators and advertisers using toll-free numbers all over the world purposefully availing themselves to the privilege of conducting business in Connecticut, even if they do not know that Connecticut exists at all?²⁰²

9.3 Playboy Enterprises v. Chuckleberry Publishing Inc.²⁰³

The defendant, Tatillo, situated in Italy, infringed the trademark of Playboy and was subject to an injunction prohibiting him to sell or even distribute his magazine “Playmen” in the U.S. and in other countries as well. Italy was one of the countries where Playboy did not successfully obtain any injunction. The Italian publisher therefore created an Italian website (<http://www.playmen.it>) and withheld that he did not at all distribute his magazine in the U.S. since he utilized a server situated in Italy.

9.3.1 Placing information on an Italian server is equivalent

¹⁹⁹ Ibid. Quote from discussion concerning the Connecticut Long-Arm Statute.

²⁰⁰ The ‘minimum contacts test’ is fulfilled if the defendant through some act purposefully avails himself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws.

²⁰¹ *Government in Cyberspace - What Jurisdiction*, NZ Institute of Public Administration (Inc.), Governance in Cyberspace Conference, 17 April 1997, presented by Michael Cronin and Bernadette Jew, at 3.21.

[Http://www.rmmb.co.nz/cybergovhtm](http://www.rmmb.co.nz/cybergovhtm)

²⁰² *Jurisdiction in a World Without Borders*, Dan L. Burk.

[Http://zeus.bna.com/e-law/cases/heroes.html](http://zeus.bna.com/e-law/cases/heroes.html) (970925)

www.student.virginia.edu/~vjolt/vol1/BURK.htm

²⁰³ United States District Court Southern district of N.Y. - *Playboy Enterprises Inc. v. Chuckleberry Publishing Inc, Tatillo Editrice*. 939 F.Supp.1032 (S.D.N.Y 1996) June 19, 1996.

[Http://www.jmls.edu/cyber/cases/playmen.txt](http://www.jmls.edu/cyber/cases/playmen.txt) (970917)

of distributing the information within the U.S.

Tatillo maintained that people in the U.S. had to visit the Italian server in order to receive the posted information, which would be similar to boarding a flight to Italy and, once there, buy the magazine, and then fly back to the U.S. again. The court agreed to the fact that the users downloaded the information from an Italian based server, but stated that such reasoning was irrelevant. The U.S. court stated: "Defendant has actively solicited United States customers to its Internet site, and in doing so has distributed its product within the United States. When a potential subscriber faxes the required form to Tatillo, he receives back via e-mail a password and user name. By this process, Tatillo distributes its product within the United States."²⁰⁴ The court also held that by inviting U.S. users to download the posted information, Tatillo caused and contributed to the distribution of the magazine within the U.S.

9.3.2 Italian publisher ordered to ignore U.S. users or shut down the site

The Italian publisher was ordered by the U.S. court not to accept American customers or shut down the website. From such a statement one can draw the conclusion that if Tatillo would not have sold to U.S. customers, and not being subjected to the earlier injunction, he would not have been subordinated American jurisdiction. In this case, however, the court found jurisdiction due to the fact that Tatillo had actively solicited U.S. customers to the Italian based site, and thereby vended the Playmen magazine within the U.S. Nevertheless, one can distinguish a bit of "territorial hesitation" from the U.S. court, since Tatillo could proceed publishing the Playmen magazine on the world wide web, as long as no subscribers were situated in the U.S. The court also mentioned the option shutting down the Internet site completely, but I doubt that such an action is effortless to perform. Tatillo could easily open up the same type of site in some other remote location where the American injunction was not obtained.

9.4 CompuServe v. Patterson²⁰⁵

This case from 1997 has been widely debated and also heavily criticized in the media. Mr. Patterson, a software designer in Houston, Texas, was found being subject to Ohio jurisdiction. He was a shareware provider, attempting to sell his programs on-line. Patterson entered into a "Shareware Registration Agreement" (SRA) with CompuServe, which is a computer

²⁰⁴ Ibid. at 1309.

²⁰⁵ United States Court of Appeals for the sixth circuit, *CompuServe, Inc. v. Richard S. Patterson, individually, and Flashpoint Development.* (No. 95-3452) July 22, 1997. [Http://www.jmls.edu/cyber/cases/patter.html](http://www.jmls.edu/cyber/cases/patter.html) (970922)

information service headquartered in Columbus, Ohio. CompuServe provided its subscribers with access to the software, or shareware, that Patterson created. CompuServe then started distributing software with a name very similar to that of Patterson's software. Patterson alleged that CompuServe was infringing his trademarks and demanded at least \$100,000 to settle his potential claims. CompuServe observed that if Patterson's allegations of trademark infringement were correct, this would threaten CompuServe's software sales revenue with a loss of approximately \$10.8 million. Therefore CompuServe sought a declaratory judgment in the federal district court for the Southern District of Ohio, in order to ascertain that no trademark infringements had been conducted.

9.4.1 A few sales via the Internet are considered sufficient contacts

Patterson required the case would be dismissed for lack of personal jurisdiction. He claimed that he had never physically been to Ohio and that he sold less than \$650 worth of his software to only 12 Ohio residents online. The court believed that Patterson had sufficient contacts with Ohio to support the exercise of personal jurisdiction. According to this case, by entering into contract with residents of foreign jurisdictions that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is considered proper.

9.4.2 Stubborn focus on the physical placement of the server

Basically, it seems like the court focused on the physical location of the CompuServe server when determining the place of sale. The court stated that it is reasonable to subject Patterson to suit in Ohio, the state which is home to the computer network service he chose to employ, since he repeatedly sent his computer software, via electronic links, to the CompuServe system in Ohio and advertised that software on the CompuServe system. The software was sent electronically from Texas to CompuServe in Ohio for their ultimate sale anywhere in the world. CompuServe in Ohio, acted as Patterson's distributor, albeit electronically and not physically.

Even though most of the sales were made to customers outside of Ohio, the court seems to have assumed that since the software was electronically stored on a server in Ohio, all the vending to Ohio customers and non-Ohio customers took place in Ohio. If a person or business conducts a business within a forum state by being a subscriber to a local ISP, and sells a product through that provider, jurisdiction is proper. In this case the server was located in Ohio, but what if the server would have been located in another state, another country or in several states, each unknown to Patterson? It has been pointed out that such reasoning may create problems, since vendors

who lease Internet space not always know the location of the servers.²⁰⁶ There is always a possibility that overloaded servers in order to eliminate congestion, automatically switch to secondary servers in other geographic locations and by doing so, the place of vending would immediately also switch to the new location. If that would have been the case, such stubborn focus on the server location may create a very unpredictable situation for the on-line vendors.

9.4.3 Possibility of “server havens” in remote locations

I believe that if the placement of the server decides whether or not jurisdiction is proper, on-line vendors may strive to use servers placed in remote “havens” which will under no circumstances file any suits. If this is the case, Internet users around the globe could really be without protection if injured by an on-line vendor since the “havens” would not assist in any way. It is not a difficult task anymore, utilizing a server placed on the other side of the world. Often the choice of server, is a choice of free capacity as well as a choice of price.²⁰⁷

9.5 Maritz, Inc. v. CyberGold, Inc.²⁰⁸

CyberGold’s site on the Internet at “www.cybergold.com” was accessible to all users in the Internet community. This Californian website contained information about CyberGold’s upcoming planned Internet service, which naturally was not operational at the time. Maritz, Inc., located in Missouri, sought a preliminary injunction against CyberGold. Maritz claimed that CyberGold infringed upon Maritz’s trademarks in violation of the Lanham Act²⁰⁹ and that the infringement caused economic harm and injury to Maritz. CyberGold requested the court to dismiss the case due to lack of jurisdiction. Maritz claimed that the injury from CyberGold’s infringement occurred in Missouri. Maritz further stated that CyberGold’s site invited Missourians to put their names on CyberGold’s mailing list in order to get up-to-date information about the company and its forthcoming Internet service. Maritz also claimed that CyberGold actively solicited customers from Missouri through the Internet advertising.

²⁰⁶ *Government in Cyberspace - What Jurisdiction*, NZ Institute of Public Administration (Inc.), Governance in Cyberspace Conference, 17 April 1997, presented by Michael Cronin and Bernadette Jew at 3.5.

[Http://www.rmmmb.co.nz/cybergovhtm](http://www.rmmmb.co.nz/cybergovhtm)

²⁰⁷ *Nätjuridik – Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 34.

²⁰⁸ *Maritz Inc. v. Cybergold* 947 F. Supp.1328 (E.D. Mo.1996).

[Http://zeus.bna.com/e-law/cases/cyb_gold.html](http://zeus.bna.com/e-law/cases/cyb_gold.html) (970925)

²⁰⁹ 15 U.S.C. Section 1125(a).

9.5.1 Minimum contacts

The Court had to decide whether or not exercise of personal jurisdiction over CyberGold would violate due process. Due process requires that there are “minimum contacts” between the nonresident defendant and the forum state before a court can exercise personal jurisdiction over the defendant.²¹⁰ The court used the “five-part test” for measuring minimum contacts. Firstly, the nature and quality of the contacts with the forum state must be considered. Secondly, the quantity of those contacts ought to be evaluated. Thirdly, the relation of the cause of action to the contacts must be determined. Fourthly, the interest of the forum state in providing a forum for its residents should be considered and fifthly, the convenience of the parties must be taken into account.

The question was, whether maintaining a website accessible to the whole world, including Missouri, was enough to exercise personal jurisdiction. The court expressed doubts as to whether old rules concerning jurisdiction could be used in novel Internet related cases. The court stated that analogies to ordinary mail and ordinary telephone calls could not be made due to the fact that the Internet is much faster and more effective. The CyberGold website was accessed approximately 130 times by users situated in Missouri. Except for the site, CyberGold claimed to have no other contacts with the state of Missouri. The site was passive, according to CyberGold.

9.5.2 The intent of setting up a site can decide whether it is classified as passive or active

The court stated that the *intent* of setting up the site was to reach all Internet users, regardless of geographic location, in order to establish a mailing list of Internet users. The court used an analogy in order to decide that the site not active. It said that if a Missouri resident mails a traditional letter to CyberGold in California requesting information from CyberGold regarding its planned service, CyberGold would have to take some active measures in order to reply, such as writing and posting a letter or equivalent. The website, which did not contain any interactivity, automatically and indiscriminately responds to each and every Internet user who accesses its website. The court therefore thought that CyberGold’s web based contacts were of such a quality and nature that they favored the exercise of personal jurisdiction over CyberGold. The motion of Maritz to dismiss for lack of personal jurisdiction was denied.

²¹⁰ This was originally expressed in *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. (1980).

9.6 Panavision International, L.P, v. Dennis Toeppen²¹¹

This case dealt with the assignment of Internet domain names, which are the equivalent of Internet Protocol (IP) addresses used to identify the operator or owner of websites. Dennis Toeppen, an individual from Illinois, registered numerous domain names at Network Solutions, Inc. which were already federally registered trademarks. He was a so-called "spoiler" or cybersquatter preventing others from conducting business on the web under trademarked names, if not paying a "ransom-fee". The dispute arose when Panavision, a company conducting business mostly in Los Angeles California, wanted to use its company name as a domain name for a website and discovered that it was not possible due to the fact that Toeppen already registered it. Since Panavision could not use the two federally registered trademarks "Panavision" and "Panaflex", it contacted Toeppen and asked him if they could use the domain names "Panavision.com" and "Panaflex.com". Toeppen replied that he would only give up the domain names if Panavision paid him \$13,000. Panavision refused to pay and filed a trademark infringement against Toeppen in May 1996. Toeppen responded by filing a motion to dismiss the case for lack of personal jurisdiction.

9.6.1 The three-part test concerning specific jurisdiction

The court conducted the three-part test for specific jurisdiction.²¹² First, the nonresident must perform some activity by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws. He would then be aware that he could be sued in this forum.²¹³ If it is a tort, jurisdiction can be found if harmful actions are intentional, expressly aimed at the forum state, and that the defendant is aware that the harm is likely to be suffered there. Secondly, the claim must be one, which arises out of or results from the defendant's forum-related activities. Thirdly, the exercise of jurisdiction must be reasonable.

The court found Toeppen subject to personal jurisdiction under the "effects doctrine" mentioned above in the three-part test. Toeppen was found to have aimed his out of state conduct at California. Panavision was harmed by Toeppen's conduct and since California is the place of business for Panavision, Toeppen must have known that the harmful effects would result

²¹¹ *Panavision International, L.P. v. Toeppen*, 945 F.Supp. 1296 (C.D. Cal. Sept. 19, 1996). [Http://www.jmls.edu/cyber/cases/panavis.html](http://www.jmls.edu/cyber/cases/panavis.html)

²¹² General jurisdiction is the case when the defendant is domiciled in the forum state or its activities there are substantial or continuous and systematic. General jurisdiction over Toeppen was not possible. Specific jurisdiction is when the defendant's activities in the forum are sufficient to establish jurisdiction for the purposes of the litigation. There is no need to be physically present in the forum state in order to apply specific jurisdiction.

²¹³ This is from *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. (1980).

there. The court specially pointed out that Toeppen did not in any way conduct business in California via the Internet, but simply running a scam directed at this jurisdiction. This fact, makes cases such as *Bensusan Restaurant Corp. v. King*, and *CompuServe v. Patterson* not analogous to this case. I believe that this case would not be treated much different by a Swedish court. As described above, Swedish law can be applied if the crime is committed towards Swedish interests, i.e. the victim is Swedish.

9.7 State of Minnesota v. Granite Gate Resorts Inc. ²¹⁴

In Minnesota, the Attorney General has taken the very aggressive position, that anyone conducting business on the net anywhere in the world is subject to jurisdiction in Minnesota if the information can be accessed and read by the residents of Minnesota. Consumer protection statutes protect those who are subject to advertisements in Minnesota and this is one reason why Minnesota strives to make foreign web editors subject to Minnesota jurisdiction.²¹⁵ In a statement from the Minnesota Attorney General one can read the following: "Warning to all Internet users and providers ... Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws".²¹⁶

9.7.1 Las Vegas Internet advertisement violated Minnesota consumer protection

In the U.S. case *State of Minnesota v. Granite Gate Resorts Inc.*, a Las Vegas on line bookmaking company was not allowed to advertise such services in Minnesota. The state of Minnesota²¹⁷ filed a consumer fraud complaint against Granite Gate Resorts, Inc. and Kerry Rogers, the president and principal officer of Granite Gate Resorts, Inc. who thereafter filed a motion to dismiss for lack of personal jurisdiction. In Minnesota, commercial sports betting and sports bookmaking is considered illegal and the Attorney General declared that by advertising in Minnesota, and by explicitly and implicitly presenting that it is lawful, the company had violated Minnesota's consumer protection.

²¹⁴ *State of Minnesota v. Granite Gate Resorts Inc.* 1996 WL 767431 (Minn. Dist. Ct., 2d Dist, Dec. 11, 1996)
[Http://www.ag.state.mn.us/consumer/news/OnlineScams/ggRespBrief.html](http://www.ag.state.mn.us/consumer/news/OnlineScams/ggRespBrief.html) (970920)

²¹⁵ *Jurisdiction Over Commerce On the Internet* by Bradley A. Slutsky,
[Http://www.kslaw.com/menu/jurisdic.htm](http://www.kslaw.com/menu/jurisdic.htm), page 5-6.

²¹⁶ Statement of Minnesota Attorney General on Internet Jurisdiction. [Http://jmls.edu./cyber/docs/minn-ag.html](http://jmls.edu./cyber/docs/minn-ag.html)

²¹⁷ Via its Attorney General Hubert H. Humphrey III.

9.7.2 A disclaimer on the website not enough to avoid Minnesota jurisdiction

An injunction was sought, preventing the company from continuing to advertise the illegal gambling services to Minnesota residents. The company argued that they had solely placed "information" concerning the gambling service and how to be part of a mailing list, on the Internet. The company claimed they had no contacts whatsoever with Minnesota. The web site even contained a disclaimer in the form of a warning specifying that viewers should contact the local authorities to make sure it was legal to participate in any of the offered off-shore sports betting via telephone. This, however, proved to be an ineffective way of restricting liability in Minnesota, since the court did not at all appreciate such an arrangement.

9.7.3 Internet advertisements more pervasive than traditional advertisements

The Internet advertisement also listed a toll-free number to call for more information about the activities and it was possible to confirm that people from Minnesota had called the number. The court also stated that the Internet advertising is available to Minnesota consumers (and to any other Internet user as well) 24 hours a day, seven days a week, 365 days a year, until taken off the site. It was also said, that for personal jurisdiction purposes, Internet advertising has the same effect as television, newspaper and yellow pages advertising. Internet advertising may even be more pervasive than other forms of advertising due to the fact that advertisements over the Internet are available to Internet users continually and constantly.

The court stated: "If national or international companies are able to seek business in Minnesota, obtain money from Minnesota consumers, claim the protection of the Minnesota courts, but escape personal jurisdiction, Minnesota consumers are essentially without redress if they are injured by an Internet advertiser--despite the fact that the consumers could have sued if the same advertisement had appeared in a national magazine or newspaper."²¹⁸

The court held that the company should not be able to seek profit from the Minnesota market, yet claim it is beyond the jurisdiction of the Minnesota courts. Since the advertisements were made in Minnesota via the Internet, the court stated it would not be unreasonable to ask that they bear the responsibilities that come with such advertising.

²¹⁸ *State of Minnesota v. Granite Gate Resorts Inc.* Page 25.
[Http://www.ag.state.mn.us/consumer/news/OnlineScams/ggRes
pBrief.html](http://www.ag.state.mn.us/consumer/news/OnlineScams/ggRes
pBrief.html)

The court therefore succumbed to the opinion that the company had sufficient minimum contacts with Minnesota to allow the exercise of jurisdiction.

It seems like Minnesota is one of the states in the U.S. which most aggressively pursue what it considers to be on-line violations of Minnesota law, by filing various lawsuits against out-of-state advertisers and ISPs.²¹⁹ Such reasoning could function as a deterrent for an expansion and development of Cyberspace. If all countries and states would file suits against foreign web-editors whenever any material found in Cyberspace does not comply with national law, it would be extremely confusing for all parties involved. If a country does not allow advertisements containing certain elements, while such elements can be found on the Internet, I see no reason to file any suit, unless the on-line advertisement specifically is targeted at this country. In the Minnesota case, it was actually proven that Minnesota residents had called the toll-free telephone number, but I am not completely certain that one could say that the company specifically directed its' website towards Minnesota simply because a toll-free number was posted. Anyone can call a telephone number, even those who live in a jurisdiction covered by the disclaimer posted on the site.

9.8 Heroes, Inc. v. Heroes Foundation²²⁰

This case does not really present any new ideas concerning personal jurisdiction and Internet activities. A charitable organization in Columbia, Heroes, sued another charitable organization in New York, Heroes Foundation, for trademark infringement. Heroes Foundation wanted the court to dismiss the complaint for lack of personal jurisdiction and improper venue. The court found that personal jurisdiction was proper. "Heroes", founded in 1964, provides financial assistance to the surviving family members of District of Columbia law enforcement officers and firefighters who are killed in the line of duty. In 1990, another organization started using the name "Heroes Foundation" in connection with its charitable activities. Heroes sued Heroes Foundation, claiming that the related names may confuse potential contributors and thus stated that it was a question of trademark infringement and unfair competition. If a person transacts business in the District of Columbia, the court may exercise personal jurisdiction over this person, as a result of the District's long-arm statute.

²¹⁹ *Jurisdiction in a World Without Borders*, Dan L. Burk.

[Http://zeus.bna.com/e-law/cases/heroes.html](http://zeus.bna.com/e-law/cases/heroes.html) (970925)

[Http://www.student.virginia.edu/~vjolt/vol1/BURK.htm](http://www.student.virginia.edu/~vjolt/vol1/BURK.htm)

²²⁰ *Heroes, Inc. v. Heroes Foundation*, Civ.96-1260 (D.C.D.C.. Dec. 19, 1996) [Http://zeus.bna.com/e-law/cases/heroes.html](http://zeus.bna.com/e-law/cases/heroes.html) (970925)

9.8.1 A website and advertisement in a newspaper is enough to exercise jurisdiction in Columbia

The court had to determine if Heroes Foundation had purposefully availed itself of the privilege of conducting activities within the District. This was based upon two facts. Firstly, a newspaper advertisement published in The Washington Post, and a website, accessible to residents in Columbia. Due to the fact that the site was not the sole contact with the forum, the court never had to determine whether the homepage alone was enough for personal jurisdiction.

The website containing the infringing trademarks ([Http://www.heroes.org/heroes](http://www.heroes.org/heroes)) invited users to donate money. Heroes Foundation claimed that the website was passive and not targeted at any specific forum, as in the *Bensusan* case. Anyone in the world with Internet access could visit the site. The court stated that anyone within the forum could gain access to the posted material, any time since it was put there.

The court found that the website and the advertisement in The Washington Post together showed that Heroes Foundation had purposefully availed itself of the privilege of conducting activities within the District, and could reasonably anticipate the possibility of being haled into court there. Therefore the court stated that jurisdiction over Heroes Foundation was proper under the “transacting any business” clause of the District's long-arm statute.

9.9 Zippo Manufacturing Co. v. Zippo Dot Com, Inc.²²¹

Zippo Manufacturing Corporation, the producer of Zippo fuel lighters among other things, filed a complaint against Zippo Dot Com, Inc alleging trademark dilution, infringement, and false designation under the Federal Trademark Act.²²² It was the usage of the name “Zippo” in the domain name that triggered this action. Dot Com demanded the court to dismiss for lack of personal jurisdiction. Dot Com operated an Internet website and an Internet news service and had obtained the exclusive right to use the domain names “zippo.com”, “zippo.net” and “zipponews.com” on the Internet. Dot Com’s contacts with Pennsylvania had almost exclusively occurred via the Internet. Dot Com’s offices, employees and Internet servers were located in California and not in Pennsylvania. However, residents of Pennsylvania were able to view the website via the World Wide Web. Dot Com had about 140,000 paying subscribers worldwide and only about 3,000 (two percent) of those subscribers were Pennsylvanian residents. Therefore one could say

²²¹ *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.* District Court for the Western District of Pennsylvania, January 16, 1997. [Http://zeus.bna.com/e-law/cases/zippo.html](http://zeus.bna.com/e-law/cases/zippo.html) (970920)

²²² 15 U.S.C. §§1051-1127

that the website was especially designed to attract viewers in all states (including Pennsylvania) and establish continuous relationships with these. Dot Com had a contract with seven Internet access providers in Pennsylvania that permitted the subscribers to access Dot Com's news service.

9.9.1 The level of commercial activity and interactivity of websites

In the Zippo case, it was discussed how the level of activity and interactivity of various websites might have an impact on whether or not jurisdiction can be established in remote states. According to the Zippo court, there are three different types of situations that should be taken into consideration. The court stated that "...the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."²²³ If the web site owners wish to avoid jurisdiction, the sites should contain as few interactive elements as possible, since solely the posting of information on a site is not always enough to be bound to a jurisdiction. It may be better to use the site to inform potential customers of traditional telephone numbers or addresses.²²⁴ Such a behavior, may still not be enough to avoid jurisdiction.

9.9.2 Entering into contract and transmitting computer files via the Internet

The first situation is when contracts are entered with residents of foreign jurisdictions, and that the parties understand that this is the case. The situation should also consist of repeated transmissions of computer files over the Internet, in order to establish personal jurisdiction. An example of such a situation is *CompuServe v. Patterson*.

9.9.3 Passive websites

The second situation is when the website is passive, and basically only displays information to anyone interested, no matter in which jurisdiction the users are located. This is not always enough to give rise to personal jurisdiction, since there is no intent to make immediate contact with viewers in any specific jurisdiction. *Bensusan Restaurant Corp. v. King* would be an example of such a passive site which was not enough to establish jurisdiction. However, one should bear in mind that the situation is likely to

²²³ *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.* at III A 2.
[Http://zeus.bna.com/e-law/cases/zippo.html](http://zeus.bna.com/e-law/cases/zippo.html)

²²⁴ *Internet Law* by Michael J. Wagner and Matthew G. Allison in *The National Law Journal*, July 7, 1997. [Http://ljextra.com/Internet/o7o7juris.htm](http://ljextra.com/Internet/o7o7juris.htm).

change, once a certain number of sales occur, or contractual relationships are established in one specific jurisdiction.²²⁵

9.9.4 Interactivity

The third situation involves interactive websites, such as in *Maritz Inc. v. Cybergold Inc.* "In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site."²²⁶

9.9.5 The Dot Com website was more than interactive

The Dot Com website was not considered to be a passive site. The court found that the site was more than interactive, and that it involved more than advertising on the Internet in Pennsylvania. It was said that if Dot Com did not wish to be subject to Pennsylvania jurisdiction, Dot Com should never have chosen to vend its services to the residents of Pennsylvania. Dot Com argued that the activities were not significant enough to establish a substantial connection with Pennsylvania, but this was rejected by the court, since the Supreme Court once stated that even a single contact can be sufficient.²²⁷ The court found it appropriate to exercise personal jurisdiction in the Zippo case.

9.9.6 Analogy between passive websites and paperback advertisements

It still seems dubious how courts would consider a non-interactive site that solely functions as an advertisement, striving to invite customers in all various jurisdictions. If it is clear that such a site is equivalent of a traditional advertisement, there may not be any proper jurisdiction due to the fact that traditionally advertising alone is not sufficient presence within a forum to support jurisdiction. It may be argued that such an analogy between sites and ads may not sustain, since (even passive) websites may be able to create greater contact than any hard-copy advertisement ever will. The *Inset Systems* court stated in 1996 that: "...unlike hard-copy advertisements ... which are often quickly disposed of and reach a limited number of potential consumers, Internet advertisements are in electronic printed form so that they can be accessed again and again by many more potential consumers."²²⁸ If the courts will succumb to such an opinion, it may be more facile to exercise personal jurisdiction for web sites exposing themselves in remote

²²⁵ *The law long arm of the law* by William S. Galkin, esq in Computer Law Observer issue No.24, March 1997, at [Http://www.lawcircle.com/issue24.html](http://www.lawcircle.com/issue24.html).

²²⁶ *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.* at III A 2. [Http://zeus.bna.com/e-law/cases/zippo.html](http://zeus.bna.com/e-law/cases/zippo.html)

²²⁷ McGee, 355 U.S. at 223.

²²⁸ *Inset Systems, Inc. v. Instruction Set Inc.* Civil No. 3:95CV-01314 (AVC). April 17, 1996.

countries. On the other hand, if the courts disagree with the analogy, it may be harder to exercise jurisdiction for non-active websites.

9.10 Cody v. Ward²²⁹

This case from 1997 concerns personal jurisdiction when e-mails, chatting and telephones were the mediums used in order to induce a person in another state to buy stocks which turned out to be worthless. Mr. Colin M. Cody, a resident of Connecticut, was persuaded (by Mr. Kevin M. Ward - a Californian resident) into buying \$196,000 worth of stocks in E. N. Phillips company (ENP). ENP was a Louisiana based company that installed video bingo games in various casino-like locations in Louisiana. Since the stock was worthless, Mr. Cody sought damages from Mr. Ward, based on fraudulent misrepresentations. Mr. Ward wanted the court to dismiss the action due to lack of personal jurisdiction on the ground that he had not engaged in any activities that would subject him to the jurisdiction of Connecticut. He contended that the long arm statute did not apply to him since he was not physically present in Connecticut when the alleged misrepresentations were made.

9.10.1 Fifteen e-mails and a four phone calls fulfills the requirement of purposeful minimum contacts with Connecticut

Mr. Ward had communicated with potential investors concerning the ENP stock via an on-line chat service, which maintains a channel for discussion of financial matters known as "Money Talk." He had posted 225 messages on-line in order to encourage people to buy or hold ENP shares. Mr. Ward claimed to have personal contacts with the management of ENP and therefore possessed very reliable information. Some of the messages were also addressed specifically to particular individuals, including Mr. Cody. During 1993 Mr. Cody purchased 101,000 shares of ENP stock for \$196,000 in reliance on materially false and misleading statements. Mr. Ward telephoned Mr. Cody in Connecticut four times to discuss the ENP stock and sent him at least 15 e-mails to his PC in Connecticut regarding the ENP stock which caused Mr. Cody to hold his ENP shares.

The court cited the Burger King case²³⁰ several times and concluded that Mr. Ward had purposefully established minimum contacts in Connecticut and that these contacts with Mr. Cody in Connecticut were substantial enough that he should reasonably have anticipated being sued in Connecticut. The court took into consideration the nature and number of Mr. Ward's telephone calls and e-mails to Mr. Cody. Contacts that are merely

²²⁹ *Colin M. Cody v. Kevin M. Ward*, 954 F. Supp. 43 (D. Conn. 1997). Feb.4, 1997.

[Http://zeus.bna.com/e-law/cases/cody.html](http://zeus.bna.com/e-law/cases/cody.html) (970925)

²³⁰ *Burger King Corp. v. Rudzewicz*, 471 U.S. (1985).

random, or accidental, do not provide an adequate basis for personal jurisdiction according to the Burger King court, but this was not the case here.

The court stated that since the requirement of purposeful minimum contacts with Connecticut was satisfied, jurisdiction was proper. It should be noted that unfortunately the court found it unnecessary to decide whether Mr. Ward's chat messages were to be seen as purposeful contacts with Connecticut, since the e-mails and phonecalls together were enough to prove this. That could have been an interesting issue.

9.11 Digital Equipment Corp. v. Altavista Technology Inc.²³¹

This case involved a dispute between two corporations over rights and commercial interests on the Internet. Both parties operated electronic services and distributed software via the Internet. Digital Equipment Corporation (Digital) brought suit against AltaVista Technology, Incorporated (ATI), for breach of a trademark licensing agreement, trademark infringement, unfair competition, and trademark dilution. Digital was the owner of the search engine called Alta Vista²³² and of all the rights in this trademark. The two companies wrote an agreement, giving ATI a license to use the word AltaVista in the corporate name, and in the URL.²³³ ATI was not, however, allowed to use AltaVista as a name of a product or service.

9.11.1 Confusingly similar websites

After a short period of time ATI's site looked similar to and even operated in the same way as Digital's AltaVista web-search service. Users hitting the ATI site could easily be deceived that they were actually visiting Digital's AltaVista search site. In the court, it was said that several hundred thousand visitors searching for Digital's Alta Vista²³⁴ involuntarily ended up hitting ATI's site instead.²³⁵ This affected advertisers who wished to put banner ads on the Digital-site, which used to have over 20 million hits per day. If the Digital Search engine did not have enough hits per day, the situation for advertisers would be completely different. Digital claimed that ATI's web site broke the above mentioned license agreement and therefore was responsible for trademark infringements. ATI wanted the court to dismiss for lack of personal jurisdiction, but the court rejected this argument.

²³¹ *Digital Equipment Corp. v. Altavista Technology Inc.* Civil Action No. 96-12192NG, March 12, 1997.

[Http://zeus.bna.com/e-law/cases/alta.html](http://zeus.bna.com/e-law/cases/alta.html) (970925)

²³² The Alta Vista search engine has been available since December 1995 at [Http:// www.altavista.digital.com](http://www.altavista.digital.com).

²³³ The URL: [Http://www.altavista.com](http://www.altavista.com)

²³⁴ [Http://www.altavista.digital.com](http://www.altavista.digital.com)

²³⁵ [Http:// www.altavista.com](http://www.altavista.com)

9.11.2 A constantly accessible website is a sign of conducting business in Massachusetts

ATI also designed a Californian website that was accessible to surfers situated in Massachusetts. The site advertised and sold ATI's software products. At least three sales to Massachusetts residents were documented. ATI claimed that three sales were relatively insignificant. Except for the website and the three sales, ATI had no further presence in Massachusetts. The court, however, found that ATI had been conducting business in Massachusetts. The fact that the website was accessible twenty-four hours a day and seven days a week to all Massachusetts residents who could access the Web, as well as the fact that ATI sold advertising space and software through its site to citizens of Massachusetts was a sign of continuing business contacts with the state.

9.11.3 Consequences of business in Cyberspace should be considered in advance

The court discussed the fact that the dispute had come about as a result of new rapidly changing technological means, and urged courts to be careful in applying traditional concepts in all situations. The reasoning of the court concerning the risks of conducting business on-line is very interesting. Since ATI had to travel considerably far in order to appear in court, it was said that this is the price of doing business on the Internet. If one acts in a way that may cause a tort in another state, the inconvenience of traveling to the court in that state should be considered before acting. I find this reasoning peculiar if it would be applied to all cases involving websites around the world, but I have reason to believe that this was not the intention of the court, since the reasoning above is valid only under the circumstances of this case.

9.11.4 Cost efficiency and jurisdiction

Another issue discussed by the court in this case, was the relationship between cost efficiency and jurisdiction. On the one hand, many companies conduct business via the Internet due to the low costs, but if they have to anticipate costs of being dragged into courts all over America, the web-based business will be much more uneconomical. On the other hand, it may be dangerous to allow that businessmen conducting business via the web, are untouchables in all jurisdictions except for the one where they are physically located.

9.12 Hall v. LaRonde²³⁶

This case holds that the use of e-mail and telephone by a party situated in New York may establish sufficient minimum contacts with California to

²³⁶ *Hall v. Laronde*, 2d Civil No. B107423(Super. Ct. No. 165615)(Ventura County) July 8, 1997. [Http://www.ljx.com/LJXfiles/laronde/laroncourt.html](http://www.ljx.com/LJXfiles/laronde/laroncourt.html) (971017)

support personal jurisdiction. Blake Hall (California) entered into contract in 1994 with Brad LaRonde (New York). LaRonde was supposed to sell licenses for the use of a computer software application that Hall had written. Hall was supposed to be compensated for every license LaRonde sold. LaRonde sold the licenses, but compensated Hall only once. Hall wanted his full compensation and filed a suit in California. LaRonde maintained that Californian courts had no jurisdiction, since sufficient minimum contacts with California were lacking.

9.12.1 E-mail and telephone calls were the only contacts between the parties

The contacts between the parties took place via e-mail and telephone. Hall had no other contacts with New York besides from the contacts with LaRonda. Hall worked on the program in California and LaRonda sold the licenses in New York. LaRonda had no other contacts with California than those with Hall. The trial court granted LaRonda's motion and ordered the case dismissed. The court of appeal of the state of California reversed the judgement from the trial court.

9.12.2 General personal jurisdiction

Personal jurisdiction may be either general or specific. Where a nonresident's contacts with the forum state are substantial, continuous and systematic, a court may assert general jurisdiction over that person. The court said that such general jurisdiction does not require a connection between the specific transaction at issue and the forum state. Hall agreed to the fact that the evidence was not enough to support general jurisdiction, but he argued that it was sufficient to support specific jurisdiction.

9.12.3 Specific personal jurisdiction

The court explained that specific jurisdiction can be affirmed when the nonresident purposefully avails himself of various forum benefits and the controversy is related to or arise out of his/her contacts with the forum. The court cited the Burger King court²³⁷, which in 1985 stated that sufficient minimum contacts for specific jurisdiction exist where a nonresident deliberately has engaged in significant activities within a state or has created continuing obligations between himself and residents of the forum.

9.12.4 Minimum contacts can be electronic

The court discussed various aspects of personal jurisdiction. It was said that all persons have an interest in not being subject to judgments of a forum with which he or she has no minimum contacts. The court succumbed to the International Shoe court²³⁸, which in 1945 said that the requirement of

²³⁷ *Burger King Corp. v. Rudzewicz* (1985) 471 U.S. [85 L.Ed.2d]

²³⁸ *International Shoe Co. v. Washington* (1945) 326 U.S. [90 L.Ed. 95, 102].

minimum contacts ensures that the assertion of jurisdiction does not violate traditional notions of fair play and substantial justice.

The court further stated that physical presence in California should not at all be determinative since the effectiveness of modern communications does not even require people leaving their offices in order to conduct business. The requisite minimum contacts can be electronic, according to the court. In this case, Hall contacted New York electronically and LaRonde contacted California electronically. The court found that LaRonde's contacts with California were more than random, fortuitous, or attenuated and that he had purposefully derived a benefit from his interstate activities. Because of this fact, it was not unfair to require that he should answer in California for any consequences that arose from his activities. Specific personal jurisdiction was proper.

9.12.4.1 People v. Lipsitz²³⁹

This case involved fraudulent and deceptive consumer sales practices. Kenneth Lipsitz used and abused the e-mail system to solicit magazine subscriptions to the worldwide Internet community, from a location in New York. Lipsitz sent friendly e-mails to various e-mail discussion groups and portrayed himself as a member, which gave a false feeling of confidence among the other users. He also sent e-mails from fictitious past customers praising Lipsitz's excellent customer service as well as the low prices. The magazines he sold rarely ever arrived, and if they did, only with a shortened subscription, often by as much as half the length of time for which the consumer had paid for. Several unsuccessful attempts were made to trace the author of the e-mails, since Lipsitz used various methods for sending anonymous e-mails, which sometimes is referred to as "spoofing". Several consumers from New York, other states and from abroad filed complaints against Lipsitz.

9.12.5 No alternative treating of Cyberspace issues

Lipsitz claimed that the court had no jurisdiction over his Internet activity. The court stated that although Internet transactions might appear to pose novel jurisdictional issues, traditional jurisdictional standards often are enough to resolve Internet jurisdictional issues. I find the courts reliance upon "old" principles quite remarkable. It was stated that for Internet consumer fraud claims, the Internet medium is irrelevant. The court stressed the importance of placing a realistic context upon Internet matters and ignore the fact that the fraud actually happened in Cyberspace. It was said that there is no reason to take a "hands off" approach because a criminal is technologically sophisticated enough to sell on the Internet. According to the

²³⁹ *People v. Lipsitz*, NY SupCt, New York County, Index No. 400945/97, 6/23/97. [Http:www.ljx.com/internet/lipsdccc.html](http://www.ljx.com/internet/lipsdccc.html) and Electronic Information Policy & Law Report July 18, 1997, Vol 2, No 28, page 773.

court, the focus in a consumer fraud claim should be upon the location of the messenger and whether the messenger delivered what was purchased.

9.12.6 Jurisdictional considerations

The court held that the first jurisdictional consideration is whether physical presence or a sufficiently close equivalent in the jurisdiction is established. The second is whether the acts performed provide sufficient minimum contacts with the forum to meet the constitutional jurisdiction test from *International Shoe v. Washington*.²⁴⁰ Lipsitz was physically located within the jurisdiction, and jurisdiction was proper since the complaints occurred within the same jurisdiction. From this case one can draw the conclusion that if a crime is committed in Cyberspace, jurisdiction may be proper at least in the jurisdiction where the criminal is physically located. The fact that Internet is the medium used is therefore irrelevant. One must keep in mind that if a suit is filed in another jurisdiction than in the one where the alleged criminal is located, jurisdiction may not be proper.

²⁴⁰ *International Shoe Co. v. Washington*, 326 U.S. (1945).

10 American cases in which jurisdiction is refused

10.1 Pres-Kap Inc. v. System One, Direct Access Inc.²⁴¹

System One Direct Access, Inc. operated a computerized airline reservation system. The server for the system, and the main business office, were located in Florida. Pres-Kap, Inc., a New York corporation, operated a travel agency in New York. All of Pres-Kap's travel businesses were conducted from the New York office. The companies entered a lease contract in December 1989 regarding the airline reservation system. Pres-Kap was allowed to use the reservation system in return of paying a monthly fee. System One delivered and installed the computer terminals in New York. In 1991 a dispute arose between the parties relating to an alleged malfunctioning of the airline reservation system.

10.1.1 Placement of server irrelevant

System One sued Pres-Kap in Florida. Pres-Kap urged the court to dismiss the case due to lack of personal jurisdiction. Pres-Kap's contacts with Florida were not numerous. Basically, the only two contacts were the monthly payments to System One in Florida and the fact that the server of the airline reservation system was situated in Florida. The trial court in Florida stated that the contacts with Florida were enough to establish jurisdiction over Pres-Kap. The District Court of Appeal in Florida was of the opposite opinion. The court cited the *Burger King Case*²⁴² which states that an individual's (A's) contract with an out-of-state party (B) alone does not automatically establish sufficient minimum contacts in the other party's (A's) home forum in order to find jurisdiction over the out-of-state defendant (B). This is the case even when the foreign defendant (B) breaches the contract. The additional factor in the case, was the location of the database. However, the court stated that the placement of the server was irrelevant. It was said that a user might not even be aware of the exact electronic location of the database. The court did not believe that such knowledge (of the database location – New York) would have made Pres-Kap anticipate being sued in New York. The court saw a pending danger in focusing too much upon the location of the database. If one would follow the Trial courts reasoning, all on-line services could be haled into court in the state where the supplier's server happens to be located. Therefore,

²⁴¹ *Pres-Kap Inc. v. System One, Direct Access Inc.* 636 So.2d 1351 (Fla. App.1994) [Http://www.jmls.edu/cyber/cases/pres-kap.txt](http://www.jmls.edu/cyber/cases/pres-kap.txt) (980211)

²⁴² *Burger King Corp. v. Rudzewicz*, 471 U.S. (1985).

contacts based on transactions over a computer network when the defendant is unaware of where the electronic transaction takes place cannot constitute minimum contacts. The court reversed the Trial court's decision and dismissed the case for lack of personal jurisdiction. This is fair, since it is not always obvious where a server is situated. Even if it is obvious, there is a danger in such reasoning. As described above, people and organizations may strive to utilize servers in countries that protect them and do not accept suits against them.

10.2 Bensusan Restaurant Corp. V. Richard B. King²⁴³

In this case from late 1996, the main question was whether the existence of a website on the World Wide Web, *alone*, could prove sufficient in order to obtain personal jurisdiction. The court found that solely a website would not be enough to exercise personal jurisdiction. Bensusan Restaurant Corp. (the creator of a jazz club in New York City known as "The Blue Note") brought an action against Richard King, (who owned and operated a small club in Columbia, Missouri, also called "The Blue Note.") alleging that King was infringing upon Bensusan's federally registered trademark "The Blue Note". King wanted the court to dismiss the complaint for lack of personal jurisdiction.

10.2.1 A general, passive website does not focus on any particular jurisdiction

Mr.King's website was located on a computer server in Missouri, and it was a so called general access site, which does not ask for any authentication or access code before entering. Basically, anyone with access to the Internet would have been able to view the site, which contained general information about the club in Missouri as well as a program of events and information regarding tickets. However, tickets for the Missouri club were not available for purchase on the site. One would have to call, reserve and pick them up in Missouri. The court stated that, by simply creating a site, one may be seen worldwide but such behavior is not equivalent of an act purposefully directed towards a specific forum state. The court also held that the simple fact that a person can gain information on the allegedly infringing product, is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product *in New York*. Mr.King was apparently not doing any of that. Mr.King's site even contained a disclaimer, stating that The Blue Note's site should not be confused with the Blue Note in New York. Noteworthy is also that the site contained a hyperlink to Bensusan's site.

²⁴³ *Bensusan Restaurant Corp. V. Richard B. King*, 937 F. Supp. 295 (S.D.N.Y, Sep 9, 1996).
[Http://www.jmls.edu/cyber/cases/bensusan.html](http://www.jmls.edu/cyber/cases/bensusan.html)

10.2.2 Three factors determining jurisdiction

Bensusan argued that, because Mr. King's site was accessible in New York (and in the rest of the world as well), he should have foreseen that surfers in the New York area were able to view the site's material. Bensusan therefore wanted restricted access to the Missouri site by technical means, allowing only users in a certain geographic regions to access the site. The court stated that solely foreseeability of an in-state consequence and a failure to prevent that consequence is not sufficient to establish personal jurisdiction. The court expressed three factors that would be of relevance, when determining whether or not jurisdiction is at hand. Firstly, one should ascertain whether or not, the site owner purposefully availed himself of the benefits of the forum state. Secondly, one should take into consideration, whether the site owner's conduct or connection with the forum state gave reasonable expectations of being haled into court there. Thirdly, one should decide whether or not the site owner has continuous and systematic business within the forum.

10.2.3 A general, passive website alone cannot subject a web-editor to other forum's jurisdictions

The court did not find personal jurisdiction in this case, due to the fact that it was not possible to ascertain any presence in New York, other than the website, that can be accessed from all over the world. This case therefore suggests that *merely* a passive website cannot make anyone subject to other forum's jurisdictions. I find it interesting that the New York court did not consider any material on the Internet that could be read in New York, subject to jurisdiction. Bensusan appealed to the U.S. Court of Appeals for the Second Circuit²⁴⁴, which in September 1997, dismissed the complaint. The "New York approach" is much less aggressive and perhaps a bit more conservative than the "Minnesota approach". A quote from the New York court, supporting such an argument would be the following text: "Creating a site, like placing a product into the stream of commerce, may be felt nationwide--or even worldwide--but, without more, it is not an act purposefully directed toward the forum state."²⁴⁵ Of course, one must bear in mind that not all the facts are exactly the same in different cases, but it is possible to see different kinds of approaches to jurisdiction in different courts.

²⁴⁴ [Http://zeus.bna.com/e-law/\(980214\)](http://zeus.bna.com/e-law/(980214))

²⁴⁵ *Bensusan Restaurant Corp. V. Richard B. King*, 937 F. Supp. 295 (S.D.N.Y, Sep 9, 1996), under C. Due Process.
[Http://www.jmls.edu/cyber/cases/bensusan.html](http://www.jmls.edu/cyber/cases/bensusan.html)

10.3 Hearst Corporation. v. Ari Goldberger²⁴⁶

This trademark infringement case from 1997 involves the question whether the court had personal jurisdiction over Goldberger because his Internet website was accessible to, and was electronically visited by, users in New York. Hearst Corporation, is the publisher of ESQUIRE Magazine since 1933. Hearst owns the trademark registration for the mark ESQUIRE. Goldberger, who lives in New Jersey and works in Philadelphia, created a website using the Internet domain name “esquire.com”. In September 1995, Goldberger registered the above mentioned Internet domain name with Internic and in June 1996, Goldberger published his website on the Internet at the address [Http://www.esqwire.com](http://www.esqwire.com). Even though no services were yet available on his site, Goldberger planned to offer law office infrastructure network services for attorneys. Thus, he had not sold any products or services to anyone in New York. It was undisputed that New Yorkers as well as users from at least 20 various states and 34 foreign countries had visited his site.

In May 1996, Hearst brought this trademark infringement action against Goldberger. It was claimed that Goldberger, by setting up the website using the above mentioned domain name, infringed on Hearst's registered ESQUIRE and ESQ. trademarks in violation of section 32 of the Lanham Act, 15 U.S.C. § 1114. Hearst also claimed that it was a matter false designation of origin, false descriptions and representations of fact, unfair competition, dilution as well as deceptive acts and practices. In July 1996, Goldberger moved to dismiss for lack of personal jurisdiction or alternatively to transfer venue.

10.3.1 A website is analogous to a traditional advertisement in a paper magazine

The court found that Goldberger's ESQUIRE Internet website was analogous to an advertisement in a national publication or magazine and thus did not constitute sufficient contacts with New York to provide the court with personal jurisdiction over Goldberger for transacting business under CPLR § 302(a)(1). This analogy was based upon the view that the Internet website in question could be viewed by people all over the world but it was not targeted at the residents of New York or any other particular state. According to the court, New York law says that advertisements in national publications are not sufficient to provide personal jurisdiction under Section 302(a)(1).

10.3.2 Jurisdiction based upon solely a website would create

²⁴⁶ *Hearst Corporation Corp. v. Goldberger*, No. 96 CIV.3620 PKL AJP, 1997 WL97097 (S.D.N.Y Feb 26, 1997)
[Http://www.ljx.com/LJXfiles/domainsuits/esqwire.html](http://www.ljx.com/LJXfiles/domainsuits/esqwire.html) (971012)

worldwide jurisdiction

The court also stated that if jurisdiction would be found on the website alone, this would lead to a worldwide personal jurisdiction over anyone and everyone who establishes an Internet website. Such nationwide jurisdiction would not be consistent with traditional personal jurisdiction case law nor would it be acceptable to the court as a matter of policy. The judge said that Hearst might have placed itself in a catch 22 situation. If Hearst would have waited until Goldberger contracted to sell his attorney support services to New Yorkers, long-arm jurisdiction²⁴⁷ might have been appropriate. Hearst did not wait long enough. The judge recommended that an out-of-state creation of an Internet website that is accessible in New York, alone, should not provide personal jurisdiction.

10.3.3 A website directed at the whole world could be equivalent of a national magazine

One can see that both in *Bensusan* and in *Hearst*, the websites did not specifically direct themselves at users in New York, and therefore the courts did not find personal jurisdiction. These cases suggest that a website alone, should not be enough to establish jurisdiction. Only when a website is aimed towards a specific state, it will be enough to grant jurisdiction. If the site is aimed at the whole world it could, according to *Hearst*, be equivalent of an advertisement in a national magazine, which often is not considered as being a contact sufficient for establishing personal jurisdiction. From this, one can conclude that it is better (from the web-editor's view) to use a passive general site, which focuses on one jurisdiction only, or a general site which is directed towards all countries. Then, it might be classified as an advertisement in a magazine and enjoy the advantages that come with it.

10.4 Cybersell, Inc., v. Cybersell, Inc.²⁴⁸

This case from December 1997 involved alleged infringing use of a service mark used in a homepage. Cybersell, Inc. (hereafter referred to as Cybersell AZ)²⁴⁹ situated in Arizona, claimed that Cybersell, Inc. in Florida (hereafter referred to as Cybersell FL)²⁵⁰ infringed its federally registered mark "Cybersell" by posting a logo on the website saying "Welcome to Cybersell!". The main question was whether such an infringement in a

²⁴⁷ The long-arm provision provides jurisdiction over a defendant who commits tortious acts outside New York causing injury in the state.

²⁴⁸ *Cybersell Inc., v. Cybersell Inc.* No. 96-17087 D.C. No. CV-96-00089-EHC filed Dec.2, 1997. [Http://cgi.ljx.com/cgi-bin/f_cat?/prod/ljextra/data/external/1997/12/9712004.c09\(980112\)](http://cgi.ljx.com/cgi-bin/f_cat?/prod/ljextra/data/external/1997/12/9712004.c09(980112))

²⁴⁹ Cybersell AZ provided Internet and Web advertising and marketing services as well as consulting.

²⁵⁰ Cybersell FL provided business-consulting services for strategic management and marketing on the web.

website solely is sufficient for personal jurisdiction in the state where the holder of the mark has its principal place of business. Except for the website Cybersell FL had no other contacts with Arizona.

Cybersell AZ filed a complaint January 9, 1996 in the District of Arizona, alleging trademark infringement. On the same day Cybersell FL filed suit for declaratory relief with regard to use of the name “Cybersell” in the U.S. District Court for the Middle District of Florida, but that action was transferred to the District of Arizona and consolidated with the Cybersell AZ action. Cybersell FL moved to dismiss for lack of personal jurisdiction. The district court denied Cybersell AZ’s request for a preliminary injunction, and granted Cybersell FL’s motion to dismiss for lack of personal jurisdiction. Cybersell AZ appealed.

10.4.1 Three-part test in order to exercise specific jurisdiction

The Court of Appeals for the Ninth Circuit used a three-part test to determine if it was possible to exercise specific jurisdiction over the nonresident defendant in this situation. The first requirement was that the nonresident had performed an act by which he purposefully availed himself of the privilege of conducting activities in the forum. The second requirement was that the claim must have arisen from this forum-related activity. The third requirement was that the exercise of jurisdiction was considered reasonable.

10.4.2 Solely a website did not trigger jurisdiction

Cybersell FL contended that a party should not be subject to nationwide, or perhaps worldwide, jurisdiction simply for using the Internet. The court stated that no court it knew of had ever held that an Internet advertisement alone was sufficient to subject the advertiser to jurisdiction in the plaintiff’s home state. Cybersell AZ claimed that a defendant should not be permitted to take advantage of modern technology through an Internet website and simultaneously escape traditional notions of jurisdiction. The court referred to the *Zippo* case and stated that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. Cybersell FL had not conducted any commercial activity through the Internet in Arizona. Except for Cybersell AZ, nobody from Arizona had ever visited the site. The website was passive, as in *Bensusan* and no 800-telephone number was posted on it, as in *Inset Systems*. The court applied the “minimum contacts” analysis, and concluded that it would not comport with “traditional notions of fair play and substantial justice” for Arizona to exercise personal jurisdiction over an allegedly infringing Florida website advertiser who had no contacts with Arizona other than maintaining a home page that was accessible to Arizonans, and everyone else, via the Internet.

10.4.3 A passive site with no commercial activities relating to the jurisdiction

The court did not have to go any further than the first part in the three-part test for specific jurisdiction. It concluded that the passive nature of Cybersell FL's activity in posting a homepage that allegedly used the service mark of Cybersell AZ did not qualify as purposeful activity invoking the benefits and protections of Arizona. As it engaged in no commercial activity and had no other contacts via the Internet or otherwise in Arizona, Cybersell FL lacked sufficient minimum contacts with Arizona for personal jurisdiction to be asserted over it. The court said that Cybersell FL's contacts were insufficient to establish "purposeful availment" and declined to go any further in the case.

10.4.4 Mc.Donough v. Fallon McElligott, Inc.²⁵¹

A photographer, Mc.Donough, sued Fallon for misappropriation of his work. Fallon sought to have the proceedings dismissed for lack of personal jurisdiction. The mere fact that Fallon's site could be accessed by Californians, was not by itself, enough to establish jurisdiction. The mere creation of a website does not provide the necessary minimum contacts with a forum state to give rise to jurisdiction there.

²⁵¹ *Mc.Donough v. Fallon McElligott, Inc.* 40 U.S.P.Q.2d 1826 SD Cal. (Aug. 5, 1996)

11 Conclusion regarding the cases involving jurisdiction

Even though the circumstances have not been exactly the same in all the cases above, it may be possible to perceive a pattern developing during 1996 and 1997. One may try to generalize the various circumstances in the cases and see if there exists any interesting legal solutions regarding Internet related jurisdiction issues that can be applied in possible future cases. What should the perfect website look like, in order to avoid being subject to jurisdiction in unwanted states or countries?

11.1 Interactivity and passivity

Merely a passive general access website cannot make a web-editor subject to other forum's jurisdictions, according to the *Bensusan* court in 1996. This reasoning was expanded by the *Hearst* court in 1997. A website may be considered analogous to an advertisement in a national publication or magazine, which generally is insufficient to exercise personal jurisdiction over the defendant. Worldwide jurisdiction as an effect of a website alone, would not be consistent with traditional personal case law, according to the *Hearst* court. The *Cybersell* court stated in December 1997, as in *Bensusan*, that a passive site should not be enough in order to exercise jurisdiction.

In the beginning of 1996, the *Thomas* court basically said that posting obscene material on a website, and allowing users in remote jurisdictions to access that material, is equivalent of transporting and distributing such material to the remote jurisdictions. This is, however, a very vague and incomplete explanation. There should have been a more detailed explanation of what role the active downloading user plays in such a situation.

Even if a website is passive, a court (as the *Maritz* court in 1996) may find that the intent of the site-owner is to conduct future business with users from foreign jurisdictions. A court may decide that the website functions as a contact (with the potential customers) of such a quality that it favors the exercise of personal jurisdiction. In 1997 the *Zippo* court basically said that in order to avoid jurisdiction, a website should contain as few interactive elements as possible. If the site is completely passive (as in *Bensusan*) it is not liable in other jurisdictions until a certain number of sales occur, or contractual relationships are established in a specific jurisdiction. The *Zippo* court further stated that by vending services via the Internet to residents in a foreign jurisdiction, it is not a question of advertising any more. A single active contact with the foreign jurisdiction in Cyberspace can lead to jurisdiction. This is also the opinion of the *Digital* court in 1997. An advertising website and three sales to customers in a foreign jurisdiction was a sign of continuing business contacts with that state. A clear message was

that if one wants to conduct business in Cyberspace, one must consider the risks of having to travel to a court in another state.

11.2 Disclaimers

If a website owner posts a disclaimer in order to avoid liability in foreign jurisdictions, as in the *Minnesota* case from 1996, it may not be enough to avoid jurisdiction. It is unfortunate that the Minnesota court did not specify the reasons for not accepting such an arrangement. With such a restrictive attitude, as in Minnesota, it seems difficult for foreign website owners to foresee the consequences and abstain from actions that may lead to being hauled into court there.

11.3 Availing oneself of the privilege of conducting business within the foreign jurisdiction

Another interesting issue is that of accessibility to a website. If one has a password-secured website and refuses to supply passwords to users in foreign jurisdictions, one certainly diminishes the risk of liability in those jurisdictions. If one intentionally gives foreign users access to a site, a court may presume, as in the *Thomas* case, that the website owner has a clear intention to avail himself to the foreign market. Other courts, as the *Inset* court, may be even more stringent and state that the mere posting of an advertisement together with an 800 number on a website is equivalent of purposefully availing oneself to the privilege of doing business in foreign jurisdictions. According to the *Inset* court, the number of users from the foreign jurisdiction actually visiting the site or calls the 800 number is of subordinated importance. The *Heroes* court found in 1996 that if a website is not the sole contact with a foreign jurisdiction, the website owner may be liable in a foreign jurisdiction. The combination of a website and a newspaper advertisement, which can be read in the foreign jurisdiction, may demonstrate that one has purposefully availed oneself of the privilege of conducting activities within the jurisdiction and therefore should anticipate being haled into court there.

11.4 The physical location of servers and databases

As early as in 1994, the *Pres-Kap* court discussed the irrelevance of physical locations of servers and databases. According to the court, contacts based on transactions via a computer network, when the defendant is unaware of the location of the electronic transaction, i.e. the server or database location, do not constitute minimum contacts. Several courts, such as the *Playboy* court and the *CompuServe* court, have rejected this idea. If one places information on a foreign server situated in e.g. Europe, U.S. courts may find that one is distributing the material in the U.S., according to the *Playboy* case from

1996. The physical placement of a server seemed to be of less importance. According to the court it seems irrelevant whether the information is stored in Europe or in the U.S. If one, however, blocks users located in the U.S. from accessing the site, one would not be considered distributing material in the U.S. and one would not be liable there. Completely different signals were sent from the *CompuServe* court in 1996. The court focused tenaciously upon the server location, but I believe that courts are beginning to comprehend that it really does not matter any longer, where the server is physically located. If courts would adamantly stick to the server location in order to find personal jurisdiction, I believe that server havens will be the next move in order to avoid jurisdiction. If one enters into contract with residents of foreign jurisdictions and knowingly transmits files repeatedly, jurisdiction may be proper.

If a person systematically snatches domain names on the Internet in order to hurt a party in a foreign jurisdiction, a court may use the “effects doctrine” as the *Panavison* court did in 1996. Since it is a matter of intentionally directing a crime towards victims in another jurisdiction, a court may find that the person is fully aware of the fact that the harmful effects will result in that foreign jurisdiction, and grant jurisdiction over him.

11.5 E-mail contacts

If one does not utilize a website but a couple of e-mail messages and a few telephone calls that are not random or accidental, in order to contact persons in other jurisdictions, it may, as in the *Cody* case from 1997, fulfill the requirement of minimum contacts. This was also the case in the *Hall* case from 1997. The court stated that physical presence is not determinative any longer. Intentional and systematic e-mail contacts and telephone calls were enough to demand the party to answer in the foreign jurisdiction. In the *Lipsitz* case from 1997, e-mail contacts in discussion groups were enough to establish jurisdiction in the state in which the “criminal” was physically located. That proves that the Internet is not a haven where people can commit crimes without being haled into court anywhere. There is often a possibility for “Internet victims” to sue the “criminal” in the state where he is physically present.

12 The role of national legal frameworks in a multinational Cyberworld

It has been argued that because there are such a great number of national laws applying to actions in the multinational Cyberspace, the legal situation is leading towards international chaos. Every country has its own legal framework relating to actions performed on the Internet. Due to the fact that information flows across the borders all the time, I believe there is an overhanging need for cooperation between governments in order to gain control over the Internet. Domestic regulation could lead to the creation of cyber havens where intellectual property infringements never will be taken to court. Finland almost became a cyber haven in 1995, when a Finn wanted to expand his anonymous remailer services, which could be used in order to act completely anonymously in Cyberspace.²⁵²

12.1 Virtual Cybercourts

There have been suggestions of creating an independent Cybercourt jurisdiction totally separated from ordinary national courts outside Cyberspace. Virtual courts should be able to arbitrate and mediate in on-line disputes. There have also been suggestions of allowing individuals to regulate the conduct on the Internet through contracts and custom such as “netiquette” were the system operators should ban anyone breaking such rules. Groups would be formed with various constitutional principles. It would then be up to each individual to choose which rules he/she is willing to accept and only access those areas in Cyberspace.²⁵³ I doubt such informally suggested solutions ever becoming reality unless there is a universal widespread consensus regarding the issue.

12.2 International Copyright Treaties

In order to harmonize national rules concerning intellectual property, several countries have accepted various international treaties. Due to the increasing exploitation of intellectual property in the on-line environment, which no longer knows any physical borders, it is very important to have internationally agreed minimum standards of protection as well as principles.²⁵⁴ The main multilateral agreements are for example the Berne

²⁵² *Government in Cyberspace - What Jurisdiction*, NZ Institute of Public Administration (Inc.), Governance in Cyberspace Conference, 17 April 1997, presented by Michael Cronin and Bernadette Jew.

[Http://www.rmmb.co.nz/cybergov.htm](http://www.rmmb.co.nz/cybergov.htm)

²⁵³ *Ibid.* chapter 7.

²⁵⁴ One important principle is the principle of equal treatment of national and foreign works.

Convention for the protection of literary and artistic works,²⁵⁵ the Rome Convention for the protection of performers, producers of phonograms and broadcasting organizations²⁵⁶ and the Agreement on Trade-Related Aspects of Intellectual Property Rights.²⁵⁷ There exist two new treaties relating to intellectual property that still have not come into force: the WIPO copyright treaty, and the WIPO performances and phonograms treaty.

One drawback with the international conventions is that questions relating to jurisdiction are normally not considered. This is not as serious as it may seem, since the legal frameworks relating to intellectual property are very alike in a number of countries.²⁵⁸

²⁵⁵ Paris Act of July 24, 1971. [Http://www.wipo.int/eng/iplcx/wo_ber0_.htm](http://www.wipo.int/eng/iplcx/wo_ber0_.htm)

²⁵⁶ Dated 1961.

²⁵⁷ Generally referred to as the TRIPs agreement of 1995.

²⁵⁸ *Nätjuridik – Lag och rätt på Internet*, by Thomas Carlén-Wendels, page 79.

13 Conclusion

It surely is most convenient if old laws can be applied to all new technological developments, such as Cyberspace, but sometimes it is not enough if one wants to cover all possible hazards to intellectual property. Since we are only in the beginning of the new information society, I believe it is of highest importance to study the technical developments as they emerge, in order to stay ahead and predict possible new legal dilemmas and reduce the lead of the pirates. If the legal systems do not recognize new complex technological problems in time, they may be unable to act as rapidly as they need in the future. Technology systems develop much faster than legal systems, and I am of the opinion that if laws are not updated and revised constantly, there is a risk that the laws could lag behind the technology, and be unable to satisfactorily protect intellectual property from piracy. However, one should not be too restrictive if one wants to see further technological developments in Cyberspace. If Cyberspace becomes too heavily regulated on all areas, there is a risk that the technological development stagnates. That would be a great loss for future generations. It would also deprive intellectual property owners of a great medium for displaying their works. The legal systems must be able to balance intellectual property protection against the technological development, without hindering either one.

Perhaps the owners of intellectual property will be forced to solely rely upon technological protection measures, thus constantly facing the risk of intellectual property pirates cracking their safety systems. If such a system brakes down, intellectual property owners could be completely without protection. I believe such technological protection systems may function as a complement to intellectual property laws. At this point in time, as far as I understand, there do not exist any technical safety measures for intellectual property that would not need the backup of laws in certain situations. I am afraid that without solid protection for intellectual property, the incentive to create may disappear, which would be a great loss to mankind. What is the economical point of creating something if it cannot be sold? Perhaps the authors will sell the first copies of their work very expensive in order to regain the predicted lost profits. After the first sales, everybody may be able to achieve the work for free in Cyberspace anyway. If intellectual property becomes even more expensive to use in the future, the incentive to upload and download unlawful copies becomes even greater.

Sources of information

Bibliography

BNA's Electronic Information Policy and Law Report, July 18, 1997, page 741 and 778.

BNA Patent, Trademark & Copyright Law Daily, June 13, 1997.

Bogdan, Michael. *Svensk internationell privat- och processrätt*, edition 4:3, Lund 1995. ISBN 91-38-50115-5.

Carlén-Wendels, Thomas, *Lag och rätt på Internet*, first edition, Stockholm, 1997.

Coughlin, Jr, George Gordon, *Your Handbook of Everyday Law*, fifth edition, New York, 1993. ISBN 0-06-271572-0.

Dag Mattson in Karnov 1996/97, page 919 at 14.

Daily Variety, June 10, 1997, page 1, by Christoffer Stern.

Electronic Engineering Times, August 11, 1997, by Brian Rost, page 115.

Electronic Information Policy & Law Report July 18, 1997, Vol 2, No 28, page 773.

Folkesson, Christina, *Skydd för upphovsrätt på Internet*, Stockholm, 1996. ISBN 91-7598-800-3.

Koktvedgaard and Levin, *Lärobok i Immaterialrätt*, Stockholm 1996, fourth edition, ISBN 91-38-50560-6.

Lindberg, Agne and Westman, Daniel, *Praktisk IT-rätt*, Stockholm, 1997. ISBN 91-38-50521-5.

PR Newswire, June 2, 1997.

Rosenoer, Jonathan, *Cyberlaw – The Law of the Internet*, Springer-Verlag New York, Inc 1997. ISBN 0-387-94832-5.

Single Market News, The Newsletter of DG XV – Internal Market and Financial Services, No 10, Dec 1997, page 22-23.

Strömberg, Håkan, *Tryckfrihetsrätt och annan yttrandefrihetsrätt*, tenth edition, Lund 1992. ISBN 91-44-00031-6.

The Guardian (London), May 16, 1997 page 12.

The Financial Post, August 28, 1997, by Alice Rawsthorn, Financial Times.

Official sources

Brottsbalken

Georgia Computer Systems Protection Act 16-9-93.1
[Http://www.mindspring.com/~ajc10/galaw.html](http://www.mindspring.com/~ajc10/galaw.html) (980215)

[Http://www2.echo.lu./legal/en/ipr/software/software.html](http://www2.echo.lu./legal/en/ipr/software/software.html) (971201).

INTA (International Trademark Association)“White Paper” - *The Intersection of Trademarks and Domain Names*, Feb 5, 1997, Version 1.0.
[Http://plaz.interport.net/int/wpwhole.htm](http://plaz.interport.net/int/wpwhole.htm) (971121)

Internic Sweden.
[Http://www.internic.se](http://www.internic.se) (971104)

Lag (1960:729) om upphovrätt till litterära och konstnärliga verk

Lag (1998:000) om ansvar för elektroniska anslagstavlor.

Paris Act of July 24, 1971.
[Http://www.wipo.int/eng/iplex/wo_ber0_.htm](http://www.wipo.int/eng/iplex/wo_ber0_.htm)

Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society, Brussels, 10.12.1997. COM(97)628 final

Prop. 1992/93:48

Prop. 1993/94:122

Prop. 1997/98:15

Statement of Minnesota Attorney General on Internet Jurisdiction.
[Http://jmls.edu./cyber/docs/minn-ag.html](http://jmls.edu./cyber/docs/minn-ag.html)

The Copyright Act §117 Limitations on exclusive rights: Computer programs. [Http://www.sgpdlaw.com/software_copyright/part1.html#117](http://www.sgpdlaw.com/software_copyright/part1.html#117) (971025)

Varumärkeslag (1960: 644)

WIPO, Issues relating to trademarks and Internet domain names. First session, Geneva, May 26 to 30, 1997.

[Http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm](http://www.wipo.int/eng/Internet/domains/tdn/cm/cm_I_2.htm)

WIPO, Consultative meeting on Trademarks and Internet Domain names, second session, Geneva, September 1 and 2, 1997.

[Http://www.wipo.int/eng/internet/domains/tdn/cm/cm_ii_2.htm](http://www.wipo.int/eng/internet/domains/tdn/cm/cm_ii_2.htm) (971025)

Electronic articles

Cache-22: Copying and storing Web pages is vital to the Internet's survival - but is it legal? By Eric Schlachter. Intellectual Property Magazine Summer 1996. [Http://www.ipmag.com/schlacht.htm](http://www.ipmag.com/schlacht.htm)

Cyberlaw: Issues in Internet Commerce, by Thomas E. Jensen.

[Http://www.cyberlaw.com/issues.htm](http://www.cyberlaw.com/issues.htm) (970724)

Dangerous Liaisons: The Legal Risks of Linking Web Sites, Richard Raysman and Peter Brown, The New York Law Journal, April 8, 1997.

[Http://www.ljx.com/Internet/0408lias.html](http://www.ljx.com/Internet/0408lias.html) (971006)

Deputizing the ISPs – Internet Service Providers should take responsibility for policing copyright infringement in Cyberspace, by William J. Cook. Intellectual Property Magazine, spring '96.

[Http://www.ipmag.com /acook.htm](http://www.ipmag.com /acook.htm) (970716)

Domain name disputes: Preemptive Suits, by Joanna Glasner. Law Journal EXTRA!, Sept. 17, 1997.

[Http://www.ljx.com/ljxfiles/domainlaw.html](http://www.ljx.com/ljxfiles/domainlaw.html) (971012)

Extending Personal Jurisdiction to Acts in Cyberspace, by Dane Steffensson for Law 7333 (Law & The Internet) spring semester 1997 at Georgia State University College of Law.

Frame Liability Clouds the Internet's Future, The New York Law Journal, May 19, 1997.

[Http://www.ljx.com/Internet/0519nyframe.html](http://www.ljx.com/Internet/0519nyframe.html) (971006).

'Framing': Internet Equivalent of Pirating?, The New York Law Journal April 4 and 11, 1997 (published in two parts)

[Http://www.ljx.com/Internet/0411frame.html](http://www.ljx.com/Internet/0411frame.html)

Freedom to Link Under Attack, The New York Law Journal, June 23 1997.

[Http://www.ljx.com/Internet/0623link.html](http://www.ljx.com/Internet/0623link.html) (971006)

Glossary.

[Http://www.glossary.com](http://www.glossary.com) (971014).

Government in Cyberspace - What Jurisdiction, NZ Institute of Public Administration (Inc.), Governance in Cyberspace Conference, 17 April 1997, presented by Michael Cronin and Bernadette Jew.
[Http://www.rmmb.co.nz/cybergovhtm](http://www.rmmb.co.nz/cybergovhtm)

[Http://www.clari.net/brad/linkright.html](http://www.clari.net/brad/linkright.html) (971021)

[Http://www.news.com/News/Item/0,4,16280,00.html?dtn.head](http://www.news.com/News/Item/0,4,16280,00.html?dtn.head) (971212)

[Http://zeus.bna.com/e-law/](http://zeus.bna.com/e-law/) (980214)

Intellectual Property, by Jeffrey R. Kuester and Daniel R. McClure, The National Law Journal, Jan 20, 1997.
[Http://www.ljx.com/internet/0120ispcp.html](http://www.ljx.com/internet/0120ispcp.html) (971006)

Internet Law by Michael J. Wagner and Matthew G. Allison in The National Law Journal, July 7, 1997.
[Http://ljextra.com/Internet/o7o7juris.htm](http://ljextra.com/Internet/o7o7juris.htm).

Internet Service Providers seek to be shielded from laws targeting pirates, by Bob Dart. The Atlanta Journal, Sept. 5, 1997, page 11A.

Internet Technology makes it hard to protect a copyright, Inside Business July 1997, by Kristen Caldwell.
[Http://www.hunton.com/in0797ib.htm](http://www.hunton.com/in0797ib.htm) (971015)

Jurisdiction in a World Without Borders, Dan L. Burk.
[Http://zeus.bna.com/e-law/cases/heroes.html](http://zeus.bna.com/e-law/cases/heroes.html) (970925)
[Http://www.student.virginia.edu/~vjolt/vol1/BURK.htm](http://www.student.virginia.edu/~vjolt/vol1/BURK.htm)

Jurisdiction Over Commerce On the Internet by Bradley A. Slutsky,
[Http://www.kslaw.com/menu/jurisdic.htm](http://www.kslaw.com/menu/jurisdic.htm), page 5-6.

Linking Copyright to Homepages, Matt Jackson.
[Http://www.law.indiana.edu/fclj/v49/no3/jackson.html](http://www.law.indiana.edu/fclj/v49/no3/jackson.html)

Linking Rights, Brad Templeton.

Ninth Circuit Uses Copyright Law to Slam Independent Service Organizations, LGU Technology Law Bulletin, July 1993.
[Http://www.lgu.com/cr47.htm](http://www.lgu.com/cr47.htm) (971024)

Oppenheim's opinion in the Shetland News Case.
[Http://www.shetland-news.co.uk/editorial/profopp1.htm](http://www.shetland-news.co.uk/editorial/profopp1.htm) (970715)

Revised Rules Govern Domain-Name Disputes, by Seyamack Kouretchian, The National Law Journal, Oct 28, 1996.

[Http://www.ljx.com/Internet/filetm.html](http://www.ljx.com/Internet/filetm.html) (971104)

Satterlee Stephens Burke & Burke LLP.
[Http://www.ssbb.com/trademar.html](http://www.ssbb.com/trademar.html) (971009)

Senate Judiciary mulls on-line copyright infringement, BNA, Patent, Trademark & Copyright Law Daily, Sept.5, 1997

Solicitation via the Internet; Jurisdiction over Claims by Edward Brodsky, The New York Law Journal, June 11, 1997
([Http://ljextra.com/Internet/061irsolic.htm](http://ljextra.com/Internet/061irsolic.htm)).

Tension Between Paralell Universes: Trademarks clash with domain names as business identify moves onto the Internet, by Mark F. Radcliffe and Maureen S. Dorney. Intellectual Property Magazine, winter 1996.
[Http://www.ipmag.com/radcliff.htm](http://www.ipmag.com/radcliff.htm) (970716)

The domain name currently called Prince, by Doughlas Hayward. Techwire 07/31/97.
[Http://techweb2.web.cerf.net/wire/news/jul/0731prince.htm](http://techweb2.web.cerf.net/wire/news/jul/0731prince.htm) (970801)

The Future of the Internet – What Role for Europe? Interim Report of an Advisory Group 970311.
[Http://www.cordis.lu/esprit/src/i2eurepo.htm](http://www.cordis.lu/esprit/src/i2eurepo.htm) (970805)

The Internet Copyright Case and its implications for users of the WWW, by Professor Charles Oppenheim, Dec.6, 1996.

The law long arm of the law by William S. Galkin, esq in Computer Law Observer issue No.24, March 1997.
[Http://www.lawcircle.com/issue24.html](http://www.lawcircle.com/issue24.html).

The Name Trade: How to deal for a domain, by Jefferson Scher, Intellectual Property Magazine, December 1996.
[Http://www.ipmag.com/scher.htm](http://www.ipmag.com/scher.htm) (970716)

The Net: Domain resellers confuses users, by Janet Kornblum, July 9, 1997.
[Http://www.news.com/news/item/o,4,12296,00.html?dtn.head](http://www.news.com/news/item/o,4,12296,00.html?dtn.head) (971009)

Tracking and Monitoring Music on the Internet, White Paper, Sept 1997, by Marco Papa, Ph.D. Chief from Intersect Inc.
[Http://www.intersectinc.com/technology.hym1](http://www.intersectinc.com/technology.hym1) (971212)

Trademarks Along the Infobahn: A first Look at the Emerging Law of Cybermarks, by Dan L. Burk, April 10, 1995, 1Rich. J.L & Tech.1(1995).
[Http://www.nlc-bnc.ca/ifla/documents/infopol/copyright/burd1.htm](http://www.nlc-bnc.ca/ifla/documents/infopol/copyright/burd1.htm) (970725)

Turning On and Turning Off: Can Merely Turning On a Computer Constitute Copyright Infringement? In the Ninth Circuit, Yes, by Ronald S. Katz and Janet Arnold Hart, *The Recorder Intellectual Property Supplement*, Autumn 1995. [Http://www.coudert.com/turnon.htm](http://www.coudert.com/turnon.htm) (971022).

Why Federal Trademark law does not protect Internet Domain names, by Jeff Wilson.
[Http://www.libraries.wayne.edu/~jlitman/pwilson.html](http://www.libraries.wayne.edu/~jlitman/pwilson.html) (971121)

Cases

Art Music France v. L'Ecole Nationale Superieure Des Telecommunications, Tribunal de Grande Instance Paris [1997]EEC97.

Bensusan Restaurant Corp. V. Richard B. King, 937 F. Supp. 295 (S.D.N.Y, Sep 9, 1996).
[Http://www.jmls.edu/cyber/cases/bensusan.html](http://www.jmls.edu/cyber/cases/bensusan.html)

Burger King Corp. v. Rudzewicz, 471 U.S. (1985).

Colin M. Cody v. Kevin M, Ward, 954 F. Supp. 43 (D. Conn. 1997). Feb.4, 1997.
[Http://zeus.bna.com/e-law/cases/cody.html](http://zeus.bna.com/e-law/cases/cody.html) (970925)

CompuServe, Inc. v. Richard S. Patterson, individually, and Flashpoint Development. (No. 95-3452) July 22, 1997. United States Court of Appeals for the sixth circuit.
[Http://www.jmls.edu/cyber/cases/patter.html](http://www.jmls.edu/cyber/cases/patter.html) (970922)

Cybersell Inc., v. Cybersell Inc. No. 96-17087 D.C. No. CV-96-00089-EHC filed Dec.2, 1997.
[Http://cgi.ljx.com/cgi-bin/f_cat?/prod/ljextra/data/external/1997/12/9712004.c09](http://cgi.ljx.com/cgi-bin/f_cat?/prod/ljextra/data/external/1997/12/9712004.c09) (980112)

Digital Equipment Corp. v. Altavista Technology Inc. Civil Action No. 96-12192NG, March 12, 1997.
[Http://zeus.bna.com/e-law/cases/alta.html](http://zeus.bna.com/e-law/cases/alta.html) (970925)

Doe v. America Online Inc., CL 97-63(Fla. Cir. Ct., Palm Beach Co.1997
[Http://www.navitus.com/icons/networklaw/case_Doe.htm](http://www.navitus.com/icons/networklaw/case_Doe.htm) (971208)

Hall v. Laronde, 2d Civil No. B107423(Super. Ct. No. 165615)(Ventura County) July 8, 1997.
[Http://www.ljx.com/LJXfiles/laronde/laroncourt.html](http://www.ljx.com/LJXfiles/laronde/laroncourt.html) (971017)

Hearst Corporation Corp. v. Goldberger, No. 96 CIV.3620 PKL AJP, 1997 WL97097 (S.D.N.Y Feb 26, 1997)

[Http://www.ljx.com/LJXfiles/domainsuits/esqwire.html](http://www.ljx.com/LJXfiles/domainsuits/esqwire.html) (971012)

Heroes, Inc. v. Heroes Foundation, Civ.96-1260 (D.C.D.C.. Dec. 19, 1996)

[Http://zeus.bna.com/e-law/cases/heroes.html](http://zeus.bna.com/e-law/cases/heroes.html) (970925)

Inset Systems, Inc. v. Instruction Set, Inc. 937 F.Supp.161 (D. Conn.1996) April 17, 1996.

[Http://zeus.bna.com/e-law/cases/inset.html](http://zeus.bna.com/e-law/cases/inset.html) (970925)

International Shoe Co. v. Washington (1945) 326 U.S. [90 L.Ed. 95, 102].

MAI Systems Corporation v. Peak Computer Inc., 991 F.2d 511 (9th Cir.1993)

[Http://www.law.seattleu.edu/chonm/Cases/mai.html](http://www.law.seattleu.edu/chonm/Cases/mai.html) (971026)

Maritz Inc. v. Cybergold 947 F. Supp.1328 (E.D. Mo.1996).

[Http://zeus.bna.com/e-law/cases/cyb_gold.html](http://zeus.bna.com/e-law/cases/cyb_gold.html) (970925)

MTV Networks v. Curry, 867 F.Supp. 1028 (C.D.Cal.1994)

[Http://www.law.seattleu.edu/chonm/Cases/mtv.html](http://www.law.seattleu.edu/chonm/Cases/mtv.html) (971026)

NJA 1996:74

NJA 1996:79

Panavision International, L.P. v. Toepfen, 945 F.Supp. 1296 (C.D. Cal. Sept. 19, 1996).

[Http://www.jmls.edu/cyber/cases/panavis.html](http://www.jmls.edu/cyber/cases/panavis.html)

Playboy Enterprises Inc. v. Chuckleberry Publishing Inc, Tatillo Editrice. 939 F.Supp.1032 (S.D.N.Y 1996) June 19, 1996. United States District Court Southern district of N.Y.

[Http://www.jmls.edu/cyber/cases/playmen.txt](http://www.jmls.edu/cyber/cases/playmen.txt) (970917)

Playboy Enterprises, Inc. v Frena, 839 F. Supp. 1552 (M.D. Florida 1993)

[Http://www.leefrog.com/E-Law/Cases/Playboy_v_Frena.html](http://www.leefrog.com/E-Law/Cases/Playboy_v_Frena.html) (971212)

People v. Lipsitz, NY SupCt, New York County, Index No. 400945/97, 6/23/97. [Http://www.ljx.com/internet/lipsdcc.html](http://www.ljx.com/internet/lipsdcc.html)

Pres-Kap Inc. v. System One, Direct Access Inc. 636 So.2d 1351 (Fla.

App.1994) [Http://www.jmls.edu/cyber/cases/pres-kap.txt](http://www.jmls.edu/cyber/cases/pres-kap.txt) (980211)

Sega Enterprises Ltd. V. Maphia.

http://www.leefrog.com/E-Law/Cases/Sega_v_MAPHIA2.html (971208)

Shetland News

<http://www.shetland-news.co.uk/opinion.html> (971006)

State of Minnesota v. Granite Gate Resorts Inc. 1996 WL 767431 (Minn. Dist. Ct., 2d Dist, Dec. 11, 1996)

<Http://www.ag.state.mn.us/consumer/news/OnlineScams/ggRespBrief.html> (970920)

Triad Systems Corporation v. Southeastern Express Co., 64 F.3d 1330 (9th Cir.1995)

<Http://www.softwareindustry.org/software/issues/docs-htm/triad-1.html>

<Http://www.law.seattleu.edu/chonm/Cases/triad.html> (District court)

United States v. Thomas 74 F.3d 701 (6th Cir.). January 29, 1996.

<Http://www.leepfrog.com/E-Law/cases>

Washington Post Company et al. V. Total News Inc., U.S. District Court, Southern District of New York, 97 Civ.1190(PKL).

<Http://www.ljx.com/Internet/totalse.htm> (971011)

<Http://www.ljx.com/Internet/complain.html> (971006)

<http://www.ljx.com/LJXfiles/ticketmaster/complaint.html> (971017)

<http://www.ljx.com/LJXfiles/ticketmaster/answer.html> (971017)

<http://www.ljx.com/LJXfiles/ticketmaster/reply.html> (971017)

World-Wide Volksvagen Corp. v. Woodson, 444 U.S. (1980).

Zeran v. America Online, 958 F Supp.1124 (E.D. Va. 1997)

<Http://www.bna.com/e-law/cases/zeran.html> (971208)

Zippo Manufacturing Co. v. Zippo Dot Com, Inc. District Court for the Western District of Pennsylvania, January 16, 1997.

<Http://zeus.bna.com/e-law/cases/zippo.html> (970920)