Henrik Spang-Hanssen

Public International Computer Network Law Issues

DJØF Publishing Copenhagen
2006

Foreword of the Author

Initially, I would like to give thanks to Bertram Ramcharan that - based on his many years of working in the U.N. environment - though a book with this content should be published and of cause also for his kind words on the back-cover of this book.

Many thanks have to go to retired U.S. colonel William Murray for proof-reading.

Thanks for great help go to librarians at the magnificent Robert Crown Law Library at Stanford University where the writing of this book was finished.

At this time should be noted, that each chapter of the book has to be regarded as a separate part on its own. Thus, the order of the chapters is somewhat fortuitous.

By this time and place should also be emphasized that this book uses two essential terms, which are vital for any discussion about the worldwide public international computer networks (the Internet). These terms can be used both on civil and criminal jurisdictions issues.

One is "*Pure Online*" incidents, which is characterized by no physical shipment or tangible things are involved, and at least one user is an alien, that is, a non-resident or a non-national. Thus, the pre-condition is "pure online" cases with an alien as a defendant with only bit-transmission as link or connection to the forum State. This term had been used in my previous publications.

This book introduces a new term "*Global Jurisdiction*" which is characterized by a State's jurisdictional rules taken on its "wording" reaches all alien cybernauts, thus making a Worldwide jurisdiction involving aliens whom can be anywhere in the world (outside the forum state). This term has to be distinguished from Universal Jurisdiction. See further chapter three, section 3.3.1, Types of Jurisdiction.

Both of these terms have come up only because of the invention of public international computer networks where acts or incidents suddenly appears to be everywhere and at the same time for anyone. Thus, from the perspective of

any court or any State these could argue being a proper court or jurisdiction.

However, Global jurisdiction is prohibited by public international law, which requires closeness (a close link) and reasonableness between the jurisdiction and the alien in question. Furthermore, under public international law any jurisdiction has to respect the sovereignty of other States and their right to self-determination of rules for and over its citizen.

Sofar public international law can be said to have been a "grenz law", but Cyberspace does not "respect" geographic drawn borders. Thus, when dealing with Cyberspace one should turn the view upside down and begin with the view – not from the perspective of a State and its borders – but from the fact that Cyberspace is global reaching and that there has to be made some division of this "global space".

Global jurisdiction under public international law does not evidently mean that a narrow community view is acceptable. The content of for example the UN Declaration on human rights and the Covenant point in the opposite direction.

On the other hand, Global jurisdiction does not seem to have special relevance outside "pure online" incidents, that is, in what is usually characterized the brick and mortar world where a State or court always can pinpoint a physical connection to the alien defendant.

This book would not have been made without encouragement from Professor in Public International Law and previous Director of the Red Cross Research Center (Henri Dunant Institute, Geneva), Jiri Toman, who probably at present time is one of the most cosmographical and cosmopolitan professors in public international law in the United States.

Stanford University, August 2006

Henrik Spang-Hanssen - Research website at www.geocities.com/hssph

The Music of the Law

I like to say we must not be tone deaf to the music of the law. There are lawyers who never do hear the law's music as they go through life. Indeed, there are those who think there is none, who think the law is just a business, one for which high fees can be charged, and maybe collected, for the necessary services only a lawyer can provide.

But if you listen and understand the law's music, to quote a former law school classmate of mine, it is a music filled with the logic and clarity of Bach, the thunder, sometimes over-blown and pompous, of Wagner, the lyrical passion of Verdi and Puccini, the genius of Mozart, Gershwin's invention, Rossini and Vivaldi's energy, and Aaron Copeland's folksy common sense, Beethoven's majesty, and unfortunately not a little of the ponderous tedium of Mahler, and the sterile intellectualism of Schoenberg.

The words you can hear to the music of the law are words of equality, justice, fairness, consistency, predictability, equity, the wrongs righted, and the repose of disputes settled without violence, without undue advantage, and without leaving either side with bitter feelings of having been cheated. It is the music sung in the world of childlike innocence in which the lion lies down with the lamb.

Perhaps it is not a world that ever was, or ever will be, but it is a world worth living toward.

Sandra Day O'Connor
Justice of the United States Supreme Court (1981-2006)

From keynote address on March 16, 2002 at the Ninety-Sixth Annual Meeting of the American Society of International Law

Table of Content

Foreword of the Author ..... **v**
The Music of the Law ..... **vii**
Table of Content ..... **ix**
Introduction **1**
Henrik's Six Steppingstones **1**
Henrik's First Base: Pure Online (cross-border) 1
Henrik's Second Base: No one owns Cyberspace 1
Henrik's Third Base: The discussion of Cyberspace issues should be limited 2
Henrik's Fourth Base: No Worldwide Jurisdiction besides Universal Jurisdiction 5
Henrik's Fifth Base: Internet protocols have become customary law 6
Henrik's Sixth Base: Computer programmers & lawyers are rule-makers for Cyberspace 7
Chapter 1 ..... **9**
Who should govern the Internet **9**
1.1. Public international law 9
1.2. The public international computer network 11
1.3. Public international law on telecommunication 13
1.4. When is a State allowed to govern 15
1.5. Telecommunication – content 18
1.6. Telecommunication-pipe lines 19
1.7. International governance – Who should govern 22
1.7.1. International Telecommunications Union 24
1.7.2. International Standards Organization 26
1.7.3. Internet Engineering Task Force 26
1.7.4. Internet Corporation for Assigned Names and Numbers 27
1.7.5. International Telecommunications Satellite Organization 27
1.8. Discussion 29
1.9. Violations 31
1.10. Final remarks 34
Chapter 2 ..... **37**
IPv6 – Possibilities of Dividing Cyberspace into Jurisdictions **37**
2.1. Introduction 37

2.2. Public International Computer Network....39
2.2.1. Public International Law....39
2.2.2. The Internet Society....43
2.2.3. The International Organization for Standardization....44
2.2.4. The Internet....45
2.3. Technique in the Public International Computer Network....49
2.3.1. Some Network Terms....58
2.3.2. Basic Requirements in the Internet Architecture Suit....62
2.4. IPv4 of 1983....64
2.5. IPv6 of 1996....69
2.6. Some differences between the two IP-versions....73
2.6.1. IP Security - Attacks....76
2.6.2. 4to6 & 6to4....83
2.7. Some differences between the two IP-versions related to jurisdictional questions....86
2.7.1. From a technical point of view....87
2.7.2. From a legislation point of view....90
2.8. Final remarks....92
Chapter 3....95
Cyberspace & Universal respectively Global Jurisdiction....95
3.1. Introduction....95
3.2. Public International Computer Networks....96
3.2.1. Technically....96
3.2.2. Public International Law....98
3.2.3. When is a State allowed to legislate and enforce?....101
3.2.4. Public Computer Network....108
3.3. Jurisdiction....113
3.3.1. Types of Jurisdiction....115
3.3.2. Universal jurisdiction....121
3.3.2.1.Universal jurisdiction over criminal acts....125
3.3.3. ABA jurisdiction rules.....128
3.3.4. Global Jurisdiction....129
3.3.4.1. Examples from Common Law....129
3.3.4.1.1. United States....129
3.3.4.1.1.1 Gator.com v. L.L. Bean, Inc. – the September 2003 Decision....134
3.3.4.1.1.2 Lakin v. Prudential Securities....138
3.3.4.1.2. U.K. - Libel....140
3.3.4.1.3. Canada – Libel....141
3.3.4.2. Example from Civil Law....143

3.3.4.2.1. Denmark 143
3.4. Discussion....145
3.4.1. Sufficient Closeness 146
3.4.1.1. Universal Jurisdiction....146
3.4.1.2. National jurisdiction 153
3.4.1.2.1. Restricted Jurisdiction 156
3.4.1.2.2. Global Jurisdiction....156
3.4.1.2.2.1. Transnational Jurisdiction 160
3.4.1.2.2.2. Specific and General Jurisdiction 160
3.4.2. Reasonableness....169
3.5. Final Remarks....172
Chapter 4 175
The Zippo Sliding Scale-Method 175
4.1. Introduction 175
4.2. Als Scan, Inc. v. Digital Service Consultants, Inc., of June 2002....176
4.3. The Zippo case of 1997....178
4.4. Web-sites (activity level catalog) – U.S. Cases....181
4.5. Cyberspace Jurisdiction 196
4.6. Conclusion....201
Chapter 5 203
Online Newspapers....203
5.1 Introduction 203
5.2. Scope....206
5.3. Rules on Cross-Border 209
5.3.1. What law has to be followed? 210
5.3.1.2. United States....213
5.3.1.2. Outside the U.S. 216
5.3.2. Where is the Newspaper published? 217
5.3.2.1. Geo-tracking 218
5.3.2.2. Customer self-identification....221
5.4. Free Speech Online 222
5.4.1. United States....223
5.4.1.1. First Amendment 226
5.4.1.2. Communications Decency Act of 1996 §230....226
5.5. Single Publication Rule & Retraction....227
5.5.1. Rules 228
5.5.1.1. Restatement Tort (Second) section 577A 228
5.5.1.2. Uniform Single Publication Model Act 229
5.5.1.3. Retraction....231
5.5.2. US case law related to Single Publication Rule....232

5.6. Cases with foreign aspects 236
5.6.1. Malaysia....237
5.6.2. Canada 237
5.6.3. United Kingdom 240
5.6.4. Australia....243
5.6.5. United States....245
5.7. The issue related to the Internet 246
5.8. Final Remarks....257
Chapter 6 259
An international dispute on the Internet - Californian Yahoo! Inc. versus France 259
6.1. Introduction 259
6.2. Facts in the Civil Case....260
6.3. Facts in the French Criminal Case 261
6.4. The French Civil Case....263
6.5. The American Civil Case 265
6.6. The Ninth Circuit's decision of January 2006 268
6.7 Comments to the decision 271
6.8. Public international law aspects 274
6.9. Final Remarks....278
Chapter 7 281
CyberCrime Convention Article 22 on Jurisdiction & Public International Law....281
7.1. To what extent can a State Claim Jurisdiction over Cybercrimes under public international law? 282
7.1.1. What is a Cybercrime? 282
7.1.2. When does a State has jurisdiction over a cybercrime under public international law? 290
7.2. Universal Jurisdiction....293
7.3. U.N. Convention Against Transnational Organized Crime 294
7.4. ICC Statute's Jurisdictional Rules 298
7.5. Jurisdiction over Satellites for data transport in Outer Space 301
7.6. The Cybercrime Convention of 23 November 2001 307
7.6.1. Crimes under the Cybercrime Convention 310
7.6.2. Jurisdiction under the Convention 316
7.7. Comments to the Cybercrime Convention 324
7.7.1. Jurisdiction....324
7.7.2. Dedere aut judicare....330
7.7.3. Double jeopardy (ne bis in idem)....331
7.7.4. Extreme foreign punishment....334

7.8. Final Remarks....336
Chapter 8....343
Certain Danish Criminal Provisions related to Cyberspace....343
8.1. Introduction....343
8.2. National Cybercrime Legislation....344
8.2.1. Brief Legislative History....346
8.3. General Danish Civil Penal Provisions on Jurisdiction....347
8.4. Certain provisions on online violations....349
8.4.1. Hacking....350
8.4.1.1. Crimes related to Gaining Profit....350
8.4.1.2. Crimes related to Peace, Privacy and Honor....353
8.4.2. Piracy....356
8.4.3. Forgery....360
8.4.4. Means of Payment....360
8.4.5. Crime relating to Sexual Morality....361
Chapter 9....365
Jurisdiction Rules of Denmark & "pure online" dealings outside the European Union on international computer networks....365
9.1. Chapter 22 of the Danish Civil Procedure Code....378
9.2. The Seven Prongs, A-G....379
9.2.1. Prong A: § 246 subsection 1, compare § 237....380
9.2.2. Prong B: § 246 subsection 1, compare § 238 subsection 2....386
9.2.3. Prong C: § 246 subsection 1, compare § 242 subsection 1....388
9.2.4. Prong D: § 246 subsection 1, compare § 243....393
9.2.5. Prong E: § 246, subsection 1, 2. sentence....399
9.2.6. Prong F: § 246 subsection 2....407
9.2.7. Prong G: § 246 subsection 3....408
9.3. Enforcement/Execution....418
9.4. Final Remarks....421
APPENDIX....423
1. U.S. States with statutes on basis of the Single Publication Model Act....424
2. U.S. States that have adopted the Single Publication Rule by case law....425
3. California Single Publication Rule....427
4. U.S. Uniform Correction or Clarification of Defamation Act ["Retraction Code"]....428
5. Alabama Retraction Statute....435
6. California Retraction Statute....436
7. Chapter 22 of the Danish Civil Procedure Code....438

8. Parallel Treaty on jurisdiction between Denmark and the rest of the E.U. 442
9. Denmark's Reservations to the Cybercrime Convention and its Protocol 459
10. Abbreviations 462
11. Bibliography 464
12. Cases 492
13. Index 510

INTRODUCTION

Henrik's Six Steppingstones

Henrik's First Base: Pure Online (cross-border)

When I deal with Cyberspace, I use the term "pure online", that is, no physical shipment or tangible things are involved, and at least one user is a alien, that is, non-resident or non-national in the State or court's forum in question.[1]

Henrik's Second Base: No one owns Cyberspace

The Internet should not belong to any single State or special group of States.

The public international computer network is something "given to mankind".

At this point should be noted that the Internet protocols (IP/TCP) was made as an open code, which means, that no one had propriety over it. Secondly, the public international computer network consists of computers and other equipment that is placed around the world and each part of this equip-

[1] HENRIK SPANG-HANSSEN, CYBERSPACE JURISDICTION IN THE U.S.: THE INTERNATIONAL DIMENSION OF DUE PROCESS 137 (Complex 5/01, Norwegian Research Center for Computers and Law, Oslo University 2001 - ISBN 82-7226-046-8 – US Congress Library 2003450386), also free downloading from research website <www.geocities.com/hssph> [hereinafter SPANG-HANSSEN-1]; and HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION 298 (DJØF Publishing, Copenhagen 2004 – 87-547-0890-1 – US Congress Library 2004441311) [hereinafter SPANG-HANSSEN-2].

ment is owned by many different people and organizations and firms.[2]

The HTTP protocol that made the use of the Internet explode was developed by an Englishman at CERN in Switzerland, Berners-Lee, who invented the World Wide Web around 1990. He dedicated the protocol to the whole world.[3] HTTP's (and thus www) purpose was to ease the interchange of information from one computer to another, thus making it possible to get information from foreign computers or networks. Thus, HTTP, which is the basis for websites, is made for the purpose of making telecommunication across borders easy and accessible on an international computer network.

Henrik's Third Base: The discussion of Cyberspace issues should be limited

At page 8 in "Cyberspace Jurisdiction in the U.S.",[4] I noted that it would be preferable for Internet users if any action on the Internet could be covered by the same rules worldwide, an International Internet Law in such a way that it didn't matter where on Earth the case was brought into court. However, this is not possible because each country has its own special local interests, politics and laws.

Therefore, my thesis is, that whenever an action on the Internet is taken and all participants live in the same country, court in that country will use the law (directly or by analogy) of that country – or the country's decision-makers will make a law to deal with the national Internet-matter. Law decision-makers will of obvious reasons not in such a "pure" national-related case accept that national law should become non-valid just because a national defendant argues that Internet had been used and should have it owns rules.

Furthermore, it is my thesis that in cases where borders are crossed and an

[2] See further, HENRIK SPANG-HANSSEN, WHO SHOULD GOVERN TELECOMMUNICATIONS ON THE PUBLIC INTERNATIONAL COMPUTER NETWORKS, Chapter to "The U.N. and the Future of International Law" in Honor of Honorable Ronald St. J. MacDonald - Edited by Bertrand Ramcharan (Publisher: Martinus Nijhoff (upcoming 2006)).

[3] Berners-Lee is now director of the World Wide Web Consortium (W3C), which aim is to ensure the www's interoperability, <http://www.ibiblio.org/pioneers/lee.html> (visited April 2003).

[4] SPANG-HANSSEN-1 *supra* note 1.

issue is dealt with in an international treaty, the rules of this treaty would also be used for the Internet case if it can be done without to much use of analogy - or small easy quick amendments might be made. I do not believe it is practical to make completely new treaties for the Internet, as that would take decades.

Therefore, my conclusion is that special International Internet Law will be needed only for areas where the Internet fundamentally has created new issues and in cases where borders have been crossed. Furthermore, no nation in the world will accept that its inhabitants can be judged and/or convicted anywhere in the world for every action on the Internet.

There has to be set up some guidance for Internet users, so they know where to expect with fairness to be sued. Thus, it would be reasonable if every court in the world before making its final decision viewed what international aspect the decision would make for people outside the jurisdiction and thus whether the decision would comply with international fair play and substantial justice.

Dealings on the Internet in "Cyberspace Jurisdiction in the U.S." page 10-11 are being divided into the following three groups:[5]

Contents of Messages

	Sent by person in country A	**Sent by person in country B**
Received by person in country A	Law of country A	*Sending electronic mail: (New) Cyberspace jurisdiction & law*
Received by person in country B	Sending by normal mail: Normal International Postage's Law/ Acts between the countries	Law of country B

[5] SPANG-HANSSEN-1 *supra* note 1, at 10-11.

Information on Web-pages

	Made by person in country A	**Made by person in country B**
Read by person in country A	Law of country A	*(New) Cyberspace jurisdiction & law*
Read by person in country B	(New) Cyberspace jurisdiction & law	Law of country B

Trade/commercial through Internet

	Vendor is person in country A	**Vendor is person in country B**
Buyer is Person in country A	Law of country A	*Delivered electronic/By downloading:* *(New) Cyberspace jurisdiction & law **
Buyer is person in country B	Tangible things: (Delivered by carrier) * "Normal" jurisdiction "Normal" law (consumer / agreement)	Law of country B

* Dilemma: two kinds of rules for e.g. selling software:
If delivered pr. ordinary mail/post => normal law and normal jurisdiction
If delivered electronic/downloading => no law and no jurisdiction

The italicized fields are of special interests when dealing with the issue of personal jurisdiction and Cyberspace/Internet.

Thus, when discussing Cyberspace and issues related to this, it is my opinion it is only worth discussing issues where the Internet fundamentally has created new issues and in cases were borders have been crossed.

In all other instances, one should regard the Internet as only an alternative to other mediums as phone, telefax etc. Thus, where the Internet is only used as an alternative to old phone-conversations or mail-order (not pure-online, see below), the issue should be dealt with by "old" rules in public international law. There is no reason to make new special Internet legislation. The old treaties on Telecommunication and Postage should cover such matters.

Especially, I hold that whenever there is a tangible good involved, there is no new issue. It is evidently only use of the Internet to mail-order something as the Internet evidently is not able to make the deliverance. Thus, the issue is

not new and there will be "old fashion" border-custom-control because the purchase has to be shipped physically.

However, the issue is new if everything is only going on on the Internet. For example if one online orders a software or music file, pays online and get the delivery by downloading the purchased.

In addition, this does not imply that there is a need for a separate jurisdiction for Cyberspace,[6] but certain issues related to Cyberspace might require national regulation to be forbidden since the issue require rules are made by the public international society – rather than national or regional - because it concerns every cybernaut, is crossborder and cannot reasonably be pinpointed to a special Nation or group of such.

Henrik's Fourth Base: No Worldwide Jurisdiction besides Universal Jurisdiction

The fact that for example content on a website on the Internet or an online newspaper article can be viewed by everyone and from everywhere, has let certain courts around the world to claim they have worldwide or "global"[7] jurisdiction, even though the content was not especially intended for the forum of the court.

However, public international law does not allow "global" or worldwide jurisdiction.

What is called "universal" jurisdiction is only allowed when the international society has accepted this[8] – and if so it will only be for a very limited and specific issue, for example War-crime or Piracy on the sea.

In public international law there are two basic requirement: (1) a link or closeness between the alien and the forum state; and (2) reasonableness. As for the first, in the perspective of Cyberspace it seem more appropriate to use

[6] As suggested by David R. Johnson & David Post, *Surveying Law and Borders – The Rise of Law in Cyberspace*, 48 STAN.L.REV 1367 (1996).

[7] See further Foreword and chapter three, section 3.3.1, Types of Jurisdiction.

[8] SPANG-HANSSEN-2 *supra* note 1, at 252-254, IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 303 (6th Edition, Clarendon Press, Oxford – ISBN 0199260710), OPPENHEIM'S INTERNATIONAL LAW 469-470 (London and New York: Longman 9th Ed., paperback edition 1996 – ISBN 0582302455).

the term "closeness" than "effect" or "target"[9]; and as for the second, in the perspective for Cyberspace is seem appropriate not only to require reasonableness but also predictability[10] from the alien's point of view, thus allowing a potential defendant to structure his primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit.

It is reasonableness in international law that is decisive.[11] Thus, what is relevant, it is not the subjective or political interest of the forum State, but the objective test of the closeness of connection, of a sufficiently weighty point of contact between the facts and their legal assessment.[12]

Henrik's Fifth Base: Internet protocols have become customary law

The Internet is not an application but a data delivery service. It uses and is defined by a pair of protocols called Transmission Control Protocol, TCP and Internet Protocol, IP (usually referred to as TCP/IP). These define how the data is partitioned and carried, and contain techniques for error control since the original Internet was designed to work on noisy, error-prone mesh networks. TCP/IP is a connection-oriented protocol meaning that it relies on getting acknowledgments of each data packet sent out.

The Internet Protocol (IP) is a network layer protocol and its task is to deliver packets of data from a source host to a destination host. Transport Control Protocol/Internet Protocol (TCP/IP) is a packet-switching protocol, which is for reliable end-to-end transport.[13]

My claim is that if professor Lawrence Lessig and several others are right that "code is law",[14] and if the TCP/IP-protocol according to the constructors of the Internet is the "Constitution of the Internet", and none of the users in

[9] SPANG-HANSSEN-2 *supra* note 1, at 242, 365-366.
[10] SPANG-HANSSEN-2 *supra* note 1, at 371.
[11] SPANG-HANSSEN-2 *supra* note 1, at 256.
[12] F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 13 & 15 (1990, Clarendon Press, Oxford – ISBN 0198252471).
[13] See further below chapter 2.
[14] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999 - ISBN 0-465-03913-8) & LAWRENCE LESSIG, THE FUTURE OF IDEAS – THE FATE OF THE COMMONS IN A CONNECTED WORLD (Random House 2001 - ISBN 0-375-50578-4).

the World (governments, international organizations and individuals) since the establishment of the protocols have demanded them changed over the last 20 years, one can fairly assert, that this international basic protocol-code for international computer network - which Lessig describe as law - has become customary international law, which can be advanced before and used by the International Court of Justice in the Hague.[15]

Henrik's Sixth Base: Computer programmers & lawyers are rule-makers for Cyberspace

The IP/TCP protocols are ruling the Internet and these are written by computer technicians.[16] The law, which is ruling Cybernaut's behavior, is made by lawyers/legislators.

When mentioning present case law from around the world to computer technicians these are often totally astonished of the court decision's world-wide range, because the technicians regard and build the Internet to be borderless.

In their opinion, the judges and legislators are totally wrong and have a totally mistaken belief of the Internet.[17]

Furthermore, legislation over public international computer networks only can be done with the cooperation of the international society of states or citizens and after discussions with computer technicians.

Thus, if effective legislation over Cyberspace is wanted, technicians, legal

[15] SPANG-HANSSEN-2 *supra* note 1, at 331-333 & 340-341.

[16] See Request for Comments (RFC) published by the Internet Architecture Board, <http://www.ietf.org/rfc.html>.

[17] Use of municipal law as a template to assess international law is unacceptable, Ian Brownlie, "*The Rule of Law in International Affairs"*, citing Gerald Fitzmaurice stating: Right and power may coincide, but they may not; they are in any case distinct concepts…the law is not obligatory because it is enforced; it is enforced because it is already obligatory; and enforcement would otherwise be illegal. Brownlie further points out that the validity of a legal order must be determined ultimately by extra-legal criteria.

scholars and legislators have to cooperate.[18]

[18] SPANG-HANSSEN-2 *supra* note 1, Chapter 35 and statement in para 35 of the Tunis Agenda for the U.N. World Summit on the Information Society, reprinted in OUTCOME DOCUMENTS (International Telecommunication Union, December 2005) at <www.itu.int/wsis/promotional/outcome.pdf> (visited July 2006)(The "management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental international organizations").

CHAPTER 1

Who should govern the Internet

By Henrik Spang-Hanssen[1]

1.1. Public international law

The Internet is a web of networks of computers around the world. A Working Group under the International Telecommunications Union (ITU)[2] has defined the Internet as the publicly accessible global packet switched network of networks that are interconnected through the use of the common network protocol IP.[3] It encompasses protocols; names and addresses; facilities; arrangements; and services and applications.

It does not belong to any State or group of States in the world.[4] Thus it

[1] I'll like to thank Professor Catherine Sandoval, High Tech Law Institute for comments to this chapter.

[2] <www.itu.int>.

[3] H. Zhao, *ITU and Internet governance*, 15 December 2004, ITU Council Working Group on the World Summit on the Information Society Geneva 13-14 December 2004, WG-WSIS-7/6 Rev 1 at <www.wgig.org/working-papers.html> (visited March 2005).

[4] State sovereignty, in its most basic sense, is being redefined - not least by the forces of globalization and international co-operation. States are now widely understood to be instruments at the service of their peoples, and not vice versa. At the same time individual sovereignty - by which I mean the fundamental freedom of each individual, enshrined in the charter of the UN and subsequent international treaties - has been enhanced by a renewed and spreading consciousness of individual rights. When we read the charter today, we are more than ever conscious that its aim is to protect individual human beings, not to protect those who abuse them, Kofi Annan, *Two concepts of sovereignty*, THE ECONOMIST, 18 September 1999 page 49 at <http://www.un.org/News/ossg/sg/stories/kaecon.html> (visited January 12, 2006).

could be argued, the Internet is something like the High Sea belonging to the international society of States and under the reign of public international law.

Public international law is the sum total of legal norms governing rights and duties of the collectivities of the ruling classes - civilized participants in international intercourse in war and peace[5] - without which it would be virtually impossible for the participants to have steady and frequent intercourse.[6] It is not rules, but a normative system that operates in a horizontal legal order.[7] Public international law is a process, a system of authoritative decision-making.[8] It deals with the conduct of nation-states and their relations with other states, and to some extent also with their relations with individuals, business organizations, and other legal entities. In its conceptions, its specific norms and standards, and largely in practice, international law functions between states, as represented by their governments.

International public law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims.[9] There is no central legislature with general law-making authority and there is no executive institution to enforce public international law.

[5] Definition from HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION - POSSIBILITIES OF DIVIDING CYBERSPACE INTO JURISDICTIONS WITH HELP OF FILTERS AND FIREWALL SOFTWARE 300 (DJØF Publishing, Copenhagen 2004 - ISBN 87-574-0890-1 – US Congress Library 2004441311) [hereinafter SPANG-HANSSEN].

[6] I.A. SHEARER, STARKE'S INTERNATIONAL LAW 14 (11th Edition, Butterworth – ISBN 0406016232).

[7] ROSALYN HIGGINS , PROBLEMS & PROCESS – INTERNATIONAL LAW AND HOW WE USE IT 1 (Clarendon Press, Oxford 1994 – ISBN 0-19-876410-3), Rosalyn Higgins, *International Law and the Avoidance, Containment and Resolution of Disputes – General Course on Public International Law*, 230 RECUEIL DES COURS 23 (1991-V).

[8] *Id*. at 267.

[9] Introduction note to Part I, Chapter 1 of Restatement (Third) of Foreign Relation Law [hereinafter REST-Foreign]. Restrictions upon the independence of States cannot therefore be presumed. *S.S. Lotus* (France v. Turkey) 1927 P.C.I.J. (Ser. A) No. 10 para. 18. Also at <www.geocities.com/hssph/Lotus.doc>.

It is to be distinguished from Private International Law or Law of Conflicts, which cover a certain State's rules on judicial jurisdiction and competence, foreign judgments and choice of law.[10] It is law directed to resolving controversies between private persons, natural as well as juridical, primarily in domestic litigation, arising out of situations having a significant relationship to more than one state.

Increasingly, public international law impinges on private international activity, for example, the law of jurisdiction and judgments and the law protecting persons.[11] Public international law is a "law of the limits" (Grenzrecht).[12]

1.2. The public international computer network

The Internet was built on the premise that nobody should be able to hinder telecommunication from end user A to end user B.[13] Thus, the main protocol

[10] Municipal law governs the domestic aspects of government and deals with issues between individuals, and between individuals and the administrative apparatus, MALCOLM N. SHAW, INTERNATIONAL LAW 82 & 100 (4th Edition, Cambridge University Press – ISBN 0521576679); IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW at chapter 2 (6th Edition, Clarendon Press, Oxford – ISBN 0199260710) [hereinafter BROWNLIE]. The International Court of Justice in the *Barcelona Traction, Light, and Power Co, Limited* (Belgium v. Spain) (Second Phase) of February 5, 1970, 1970 I.C.J. 3, referred to the rules generally accepted by municipal legal systems, not the municipal law of a particular state. As for England, see PETER NORTH & J.J. FAWCETT, CHESHIRE AND NORTH'S PRIVATE INTERNATIONAL LAW 13 (3rd Ed. 1999 – ISBN 0-406-90596-7).

[11] Comments to § 101 of REST-Foreign *supra* note 9. On certain nations, see JOHN H MERRYMAN, THE CIVIL LAW TRADITION: EUROPE, LATIN AMERICA, AND EAST ASIA (The Michie Company 1994 – ISBN 1-55834-180-3).

[12] Footnote 78 in Catherine Kessedjian, *Report on International Jurisdiction and Foreign Judgments in Civil and Commercial Mattes*, Hague Conference on Private International Law - Enforcement of Judgments - Prel. Doc. No 7 - Revised Translation of October 1997, at <ftp://ftp.hcch.net/doc /jdgm_pd7.doc> (visited November 2003).

[13] One of the creators of the Internet protocol, Vinton Cerf has stated to be fearful that the phone companies that own the network of lines and cables will charge Internet companies for delivering content and thus make a set of restrictions that will hinder the consumers of content. He points out that in the Internet world, both ends essentially pay for access to the Internet system, and so the providers of access get compensated by

for the Internet (IP) uses a packet switching system that secure a communication reaches its destination. The first computer network was involving servers placed in United States, Norway and England.[14] Thus, the computer network has from the very beginning been an international network.

Another vital aspect of telecommunications on public international computer networks is the use of the HTTP protocol that was developed by an Englishman working in Switzerland. Berners-Lee, who invented the World Wide Web around 1990, dedicated the protocol to the whole world.[15] HTTP's (and thus www) purpose was to ease the interchange of information from one computer to another, thus making it possible to get information from foreign computers or networks. Thus, HTTP, which is the basis for websites, is made for the purpose of making telecommunication across borders easy and accessible on an international computer network.

This shows that the inventors of the IP protocol and HTTP wanted to make a borderless and international public computer network where people could get access to information on foreign computers and thus exchange point of views.[16]

the users at each end. The big concern is that suddenly access providers want to step in the middle and create a toll road to limit customers' ability to get access to services of their choice even though they have paid for access to the network in the first place, Vinton Cerf to Arshad Mohammed, *Verizon Executive calls for end to Google's "Free Lunch"*, WASHINGTON POST.COM, February 7, 2006 at <www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html> (visited February 8, 2006).

[14] *History - ARPAnet 1957 – 1990*, at <http://www.jmusheneaux.com/21bb.htm> (visited December 21, 2005); *A Note on the Internet* page 2, Graduate School of Business, Stanford University 1996, at <www.stanford.edu/group/scip/Afeche-internet.pdf> (visited December 21, 2005). A map showing the international underwater cables used for international Internet traffic as of the end of 2004 can be found at <http://news.com.com/2300-1033_3-6035611-1.html> (visited May 2006).

[15] Berners-Lee is now director of the World Wide Web Consortium (W3C), which aim is to ensure the www's interoperability, <http://www.ibiblio.org/pioneers/lee.html> (visited April 2003). See further SPANG-HANSSEN *supra* note 5, at 2 and *American Civil Liberties Union v. Reno*, 929 F.Supp 824, 836 para. 35 (E.D.Pa. 1996) and *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 483 (E.D.Pa. 1999).

[16] Jeff Groff, who worked with Mr Berners-Lee on the early code, has stated that a very simple idea was behind the web in 1991; and now in 2006 the web may be worldwide

Thus, this computer network was not made to belong to any special State or group of nations, but was intended to belong to the whole world.

It can therefore with good reason be argued that the Internet should be governed by the international society.

In "A Framework for Global Electronic Commerce" is stated: "The Global Information Infrastructure ("GII"), still in the early stages of its development, is already transforming our world…As the Internet empowers citizens and democratizes societies it is also changing classic business and economic paradigms…One of the principles that the U.S. believes should be the foundation for government policy... [is] guaranteeing open access to networks on a non-discriminatory basis, so that GII users have access to the broadest range of information and services."[17]

Former U.S. President Regan commented on the relationship between information systems, individuals and States: "technology will make it increasingly difficult for the states to control the information its people receive…The Goliath of totalitarianism will be brought down by the David of the microchip."[18]

1.3. Public international law on telecommunication

"Telecommunications" means the technology of carrying information by electrical and electronic signals[19] or the electronic transmission of information chosen by the sender between or among places also chosen by the sender. The definition embraces a universe of different services and technolo-

but it is only just getting started. The original conception was for a medium that people both read and contributed to. New tools such as photo-sharing sites, social networks, blogs, wikis and others are making good on that early promise, Mark Ward, *How the web went world wide*, BBC NEWS 3 August 2006 at <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/5242252.stm> (visited August 2006).

[17] William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 4, 1997) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (visited Nov. 21, 1997).

[18] Ronald Reagan in speech at London's Guildhall (June 14, 1989).

[19] MARK R. CHARTRAND, SATELLITE COMMUNICATIONS FOR THE NONSPECIALIST 37, 103 (Spie Press 2004 – ISBN 0-8194-5185-1) [hereinafter CHARTRAND].

gies. As telecommunications have become automatic and rely less on human intervention, the ability to complete transmissions across borders depends mainly on achieving compatibility among different kinds of terminal equipment and private and public networks.[20]

Data, also called digital, is the fastest growing segment of telecommunications traffic. In the first half of this decade, data traffic surpassed voice traffic, and telephony is now less than 10% of total data traffic. Data is not in itself a service. Rather, it is a way of sending the information contained in an application; and data may be carried over terrestrial or satellite-based telephone networks, over public or private terrestrial data networks, or over satellites.[21]

There exist no treaties, which require a freedom of speech combined with a right to cross-border telecommunication. However, there exist some international declarations that suggest such a regime. For example, the Universal Declaration of Human Rights states in Article 19:[22] "Everyone has the right to freedom of opinion and expression: this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Furthermore, there exists the International Covenant on Civil and Political Rights that states in Article 19:[23] "(1) Everyone shall have the right to hold opinions without interference. (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. (3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national

[20] CHARLES H. KENNEDY, AN INTRODUCTION TO INTERNATIONAL TELECOMMUNICATIONS Law 3 & 37 (Artech House Inc. 1996 – ISBN 0-890068356).

[21] CHARTRAND *supra* note 19, at 3.3.4., OPPENHEIM'S INTERNATIONAL LAW 842 (London and New York: Longman 9th Ed., paperback edition 1996 – ISBN 0582302455) [hereinafter OPPENHEIM].

[22] Adopted by UN General Assembly Resolution 217A (III) of 10 December 1948.

[23] Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976, U.N.T.S. No. 14668, vol. 999 (1976), p. 171.

security or of public order (ordre public), or of public health or morals.

However, this declaration does not mean under public international law that free speech cannot be limited by a nation through legislation.[24] Thus, under public international law, nations are to a certain degree allowed to impose limits on people's right to publish their opinions, especially if it is related to national security or cultural and on religious issues, which are often mentioned in a nation's constitution.

On the other hand as for free speech and international public law, there exists no international law stating a nation's citizen has to cut off content that is legal in at least one foreign nation besides the citizens own nation - and thus probably acceptable to the U.N. Declaration of Human Rights on free speech. Thus, public international law does not prohibit a citizen from uploading speech or information sent from a country where the content is permitted but accessed by a citizen in a country where the content is prohibited.

The Internet's ever-changing technology also makes it very difficult – if not impossible - to govern the Internet and its users. The Secretary-General of the United Nations stated in 2003, "few manifestations of the power of human creativity have so extensively and so quickly transformed society as the rise of the Internet over the past decade. Dramatic as the changes may be, the process of assimilating and learning from them has only just begun." U.S. Supreme Court Justice Souter has remarked that "we should be shy about saying the final word today about what will be accepted as reasonable tomorrow…In my own ignorance I have to accept the real possibility that…if we had to decide today…just what the First Amendment should mean in cyberspace…we would get it fundamentally wrong."[25]

1.4. When is a State allowed to govern

No laws of no nation can justify extend beyond its own territories, except so

[24] Confer Article 19(3) of UN International Covenant on Civil and Political Rights, Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976.

[25] *Denver Area Educational Telecommunications Consortium, Inc. v FCC*, 518 U.S. 727, 777 (U.S. 1996).

far as regards its own citizens. They can have no force to control the sovereignty or rights of any other nation, within its own jurisdiction.[26]

International public law on jurisdiction to prescribe in relation to international computer networks can be summed up as in the table below for Pure Online cross-border & the Nationality[27] and Territorial[28] Principles. It should be added to the table that the Subjective Territoriality Principle[29] allows State D to prescribe in all of the fields, whereas the Active Personality Principle[30] allows the State of nationality or residency of the suspect to prescribe in all of the fields.[31]

	Made online from State D by national of state A	**Made online from State D by national of State C, but citizen of A**	**Made online from State D by national of State B**
Uploaded in State E	International Law involved State E regarded as sender or receiver state?	International Law involved State E regarded as sender or receiver state?	International Law involved State E regarded as sender or receiver state?

[26] Justice Story in *The Apollon*, 22 U.S. 362, 370 (U.S. 1824).
[27] The Nationality principle confers jurisdiction over nationals of the State concerned.
[28] The Territoriality Principle confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place.
[29] The Subjective Territoriality Principle permits a State to deal with acts that originated within its territory, but was completed or consummated abroad.
[30] The Active Personality Principle is based on the nationality of the suspect. Public international law accepts jurisdiction over a state's owns citizens based on nationally, or the links between the individual and the state.
[31] See further HENRIK SPANG-HANSSEN *supra* note 5, at 300.

	International Law involved	International Law involved	International Law involved
Received in State B	Objective[32] and Passive[33] personality (controversial) principles allow State B to prescribe?	Objective and Passive personality (controversial) principles allow State B to prescribe?	

Table 1.1: Public International Law Principles involved

This implies for online communication that it has to meet the requirements of the legislation in:[34]

- The State from where the original electronic communication ("bits-transfer") was prepared
- The State where the communication is uploaded
- The State of the communicator's "nationality," that is, for a private owned communication firm where the owner is born, or a corporate is incorporated
- The State where the communicator is a "citizen," that is, for a private owned communication firm where the owner living or a corporate is having headquarter

From the receiver site's perspective,35 it should initially be noted that as the Passive personality principle generally is rejected by the international society, the communicator does not have to follow the legislation (statutes or case law) in the state of which the receiver is a nationality. However, the online communicator might have to meet the requirement pursuant to the Objective territoriality principle that permits a State to deal with acts which originated abroad but which, at least in part, were

- consummated or completed within their territory (the "effect doc-

[32] The Objective Territoriality Principle permits a State to deal with acts which originated abroad but which, at least in part, were (i) consummated or completed within their territory – the "Effect Doctrine"; or (ii) producing gravely harmful consequences to the social or economic order inside their territory - the "Protective Theory".

[33] The Passive personality principle or passive nationality principle - based on nationality of the victim, not the nationality of the offender.

[34] SPANG-HANSSEN *supra* note 5, at 345.

[35] *Id.* 346.

trine"); or

- producing gravely harmful consequences to the social or economic order inside their territory (the protective theory).[36]

The above mean that a State cannot interfere with what is going on the Internet or on the international network's "pipe-lines" through which the electronic bits of the telecommunication is transmitted. Thus, some international entity is necessary to govern the international networks of computers.

1.5. Telecommunication – content

If the above mentioned does not allow a State to prescribe, the State cannot pursuant to international law make any ruling over telecommunication in the sphere called the Internet, which is often illustrated as a cloud in an effort to demonstrate that the information is somewhere in the network on a computer or a fortuitous proxy-server and accessible for everyone from everywhere.

The latter clearly imply that each State's legislators and enforcement has to take great consideration to other State's interests, which always has been the basis for public international law.

Thus, it follows that as telecommunications in form of exchange of ideas and information is done on the public international networks and the exchange crosses State-borders, no single nation can by legislation decide what content is legal. Rather, a State can only decide what content its own citizens legally should be allowed to receive through their own "earth station" (laptop, mobile phone, flat screen). The public international network cannot be legislated as it is under the "control" of public international law, because the international society does not allow a State to make legislation that lowers the functionality of the IP-protocol and thus the packet-delivery of information on the Internet.

At the same time, the Internet has created new problems for communicators. The laws developed for speech in the brick and mortar world do not

[36] The protective theory covers a variety of political offences and is not necessarily confined to political acts. The principle is well established and seems justifiable because it protect a state's vital interests. However, it can easily be abused. The decisive is the importance of the offence, which standard is supplied solely by international law.

adequately address the public international computer networks. Opposite the situation in the brick and mortar world communicators now can expect their communication to become available everywhere and to everyone unless they do something that hinders some people access to their communication, or use one-to-one communication like e-mail (though e-mail can be easily forwarded to others). The exchange is often explained as happening in a cloud. If they do not hinder access they can expect liability claims from persons around the whole world that might have been hurt, because the receiver comes from a different culture, religion etc. Thus, the communicator's free speech rights in his own nation might not protect him, if the receiver is outside the communicator's nation and that nation's legislation support remedies or criminal prosecution.

Thus, under public international law, most Internet-telecommunication is not under control of any fortuitous State as in practice most of the information on the Internet is placed on servers outside the State in question.

1.6. Telecommunication-pipe lines

The Internet is not an application but a data delivery service. It uses and is defined by a pair of protocols called Transmission Control Protocol, TCP and Internet Protocol, IP (usually referred to as TCP/IP). These define how the data is partitioned and carried, and contain techniques for error control since the original Internet was designed to work on noisy, error-prone mesh networks. TCP/IP is a connection-oriented protocol meaning that it relies on getting acknowledgments of each data packet sent out. The Internet Protocol (IP) is a network layer protocol and its task is to deliver packets of data from a source host to a destination host.

If professor Lawrence Lessig[37] and several others are right that "code is law", and if the TCP/IP-protocol according to the constructors of Internet is the "Constitution of the Internet", and none of the users of the World (gov-

[37] Lawrence Lessig, *Legal Issues in Cyberspace: Hazards on the Information Superhighway: Reading the Constitution in Cyberspace*, 45 Emory.L.J. 869, 899 (1996) and LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999 - ISBN 0-465-03913-8).

ernments, international organizations and individuals) since the establishment of the protocols has demanded it changed, one could fairly assert, that this international basic protocol-code for international computer network, which Lessig describe as law, has become customary international law,[38] which then can be advanced before the International court of Justice in Hague.[39]

Even though the present version IPv4 has become a standard and maybe customary law, there has already been made a new version of the IP-protocol,[40] since the IPv4 has many serious limits that a new version from 1996 (IPv6[41]) has been designed to overcome. IPv6 provides a larger address space than IPv4 (128 bits in length to 32 bits), which latter only supports about 2.000.000.000 addresses and with an enormous waste of usable addresses. IPv6 uses a wiser address allocation policy – so-called Classless Inter-Domain Routing (CIDR) - which minimizes the growth of routing tables, and provides more than a billion of billions addresses per square meter on the Earth.

The number of fields in the IPv6 packet header is reduced from IPv4 (8 versus 12). The IPv6 packet header is fixed-length size with a length of 40 octets, whereas the IPv4 header is variable-length. Thus, routers have less processing to do per header, which should speed up routing.

The IPv6 design simplifies processing. In IPv6, fragmentation may only be performed by the source. In addition, the IPv6 has been designed to satisfy the growing need of security by allowing the receiver to be reasonably sure about the origin of the data with use of end-to-end encryption of data at the network layer. IP spoofing attacks and eavesdropping of data will be much more difficult. However, network-level encryption poses new security prob-

[38] Pursuant to STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW as amended at the 2000 London conference (International Law Association) nr. 11 page 19 customary law can be created by international organizations. The organs behind the TCP/IP-protocol can fairly be recognized as such international organizations, <http//:www.ila-hq/pdf/CustomaryLaw.pdf>.

[39] SPANG-HANSSEN *supra* note 5, at 341.

[40] See also *ITU and its Activities: Related to Internet-Protocol (IP) Networks, Version 1.1*, April 2004 at <http://www.itu.int/osg/spu/ip/itu-and-activities-related-to-ip-networks-version-1.pdf> (visited March 2006).

[41] William Stallings, *IPv6: The New Internet Protocol* at <http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stalings> (visited February 2005).

lems. Another problem is that decryption puts a considerable overload on the CPU and leaves the host more vulnerable to flooding-type DoS attacks.

The new IPv6 protocol gives a few possibilities in its new header to make determination of the sender. It allows use of a provider-based global unicast address, which provides for global addressing across the entire universe of connected hosts. IPv6 accommodates local-use unicast addresses, that is, packets with such addresses can only be routed locally, or within a subnetwork or set of subnetworks of a given subscriber. This should not be against public international law as a State always has had the right to determine whether information can be imported to that State's own citizens. However, it will probably require a great force of people to keep a filter in function.

IPv6 also allows a subscriber to use multiple access providers, which might make it harder for States to trace and censure a certain cybernaut's telecommunications.

However, as it is not practical to simply replace all IPv4 routers in the Internet or a private Internet with IPv6 routers - and replace all IPv4 addresses with IPv6 addresses - and as the new IPv6 has not been implemented by very many people, experts expect it to take a least ten years before a significant part of the international computer network has changed from IPv4 to IPv6. Thus, there will be a lengthy transition period where the two protocols will coexist. Such a long change-period will allow IPv6 to become customary international law, fully or partly.

As for the copper-phone-lines, satellites are also only part of the "pipe" lines for the international public networks and a State is thus not allowed to hinder or interfere data-delivery designated between two foreign States by passing another State's territory including airspace. From above section 1.4, can be concluded that a State has the right under public international law to make legislation over or totally forbid Earth stations in its territory to communicate with satellites. Under international law the territory includes the air space above, but there is no definite km-limit. On the other hand, public international law does not allow a State to legislate or make enforcement on satellites, and the telecommunication that is offered by a certain satellite if the

satellite is not in a to narrow distance from the Earth.[42] (It should be noted, the State in which the owner of a satellite is located or incorporated of cause can give binding orders to that owner). Except for satellites in the Clarke Orbit,[43] which is govern internationally by the ITU,[44] anyone can launce a satellite into orbit and offer telecommunication including the information that can be achieved from the international computer networks.

Thus, under public international law most Internet-telecommunication are not under any control of any fortuitous State as in practice most of the information is only in "transit" through the "pipe-line" of that state in form of a bit send from a foreign country A to country B.

1.7. International governance – Who should govern

On basis of the above mentioned one should ask who should govern the Internet consisting of a data-deliverance and information-exchange. Internet governance was one of the most controversial issues debated during the whole process of preparation for the U.N. World Summit on the Information Society (WSIS) partly because sovereignty is an issue that often arises, implicitly or explicitly, in debates on Internet Governance.

The ITU Working Group on Internet Governance (WGIG) has defined "Internet governance" as follows:[45]

[42] BROWNLIE *supra* note 10, at 105, 255-259, OPPENHEIM *supra* note 21, at 479, 650, 662, 826-845, and D.J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 244 (5th Edition, Sweet & Maxwell, ISBN 0-421-53470-2Hb).

[43] Geosynchronous Orbit Satellites (GSOs) are launched into a band 35,786 (22,300 miles) in altitude above Equator where it moves in consonance with the terrestrial globe and therefore is constantly over the same point. Three GSO-satellites can cover the total surface of the Earth. However, a GSO satellite cannot see any areas with latitude more than 77^{o} north or south. OPPENHEIM *supra* note 21, at 841.

[44] Because the Clarke Orbit is only of 265,000 km in range is requires an administration of this "limited natural resource" like the radio frequencies also administrated by ITU.

[45] Nitin Desai, *Annex to Preliminary Report of the WGIG – Introduction,* Chairman of the Working Group on Internet Governance (WGIG) in Geneva on 24 February 2005 at <http://www.wgig.org/docs/outline-24-11-04.pdf>. See also, H. Zhao, *ITU and Internet Governance* section 4.1(b), 15 December 2004, ITU Council Working Group on the World Summit on the Information Society Geneva 13-14 December 2004, WG-

- Descriptive – Internet governance means the collective rules, procedures, and related programs intended to shape social actor's expectations, practices, and interactions concerning Internet infrastructure and transactions and content
- Prescriptive – Internet governance should be multilateral, transparent and democratic, with the full and balanced involvement of governments, the private sector, civil society and international organizations.

It should encompass both technical and public policy aspects, ensure an equitable distribution of resources, facilitate access for all, and maintain the stable and secure functioning of the Internet, taking into account multilingualism.

The WSIS has made a Declaration of Principles for Internet Governance, which in part states:[46]

- We declare our common desire and commitment to build a people-centered, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.
- We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and

WSIS-7/6 Rev 1 and Houlin Zhao, director of TSB, ITU, address on Internet Governance at Cairo May 5, 2004.

[46] WSIS Declaration of Principles of 12 December 2003, WSIS-03/Geneva/Doc/4-E.

no one should be excluded from the benefits the Information Society offers.

- Everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society…may in no case be exercised contrary to the purposes and principles of the United Nations.
- The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.
- The Information Society should be founded on and stimulate respect for cultural identity, cultural and linguistic diversity, traditions and religions, and foster dialogue among cultures and civilizations.
- It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights.
- Upholding the principle of the sovereign equality of all States.

The above summarizes the main issues that have to be taken into consideration when considering which organ or institution is best suited to govern the Internet.

In this context, one should consider whether one or more of the existing international institutions are suited to govern the Internet. The following institutions come to mind.

1.7.1. International Telecommunications Union

The electronic radio spectrum is allocated primarily by a United Nations organization called the International Telecommunications Union (ITU).[47]

[47] <www.itu.int>. The Constitution and the Convention is included in Collection of the basic texts of the ITU (1999) at <http://www.iut.int/aboutitu/BAsic_Text_ITU-e.pdf>

There are three Sectors of the ITU: the Radiocommunication Sector (ITU-R), the Telecommunication Development Sector (ITU-D)[48] and the Telecommunication Standardization Sector (ITU-T),[49] which all work to build and support tomorrow's networks and services.[50] It interprets the Radio Regulations, sets policies for registering frequency uses, and maintains the Master International Frequency Register and the Table of Frequency Allocations.

ITU has treaty status, meaning that the provisions of the ITU's Constitution and Convention are binding on ITU member countries. However, it is only a policy organization and has no enforcement powers. It decides policies based on one-nation, one-vote, and any nation willing to adhere to its rules may join. Any member may object to adhering to any specific regulation by filing an "exception" to the rules. The supreme governing body of the ITU is the Plenipotentiary Conference, and meets every four years. ("plenipot"). The ITU has recently opened up its procedures to input from telecommunications firms and other nongovernmental organizations, although only the nation members may vote.

The ITU considers the world divided into three large geographic regions. Regulations and standards may be set differently in different regions, set the same in two regions, or even set globally.

ITU-T deals mostly with communications traveling through wires and optical fibers. It has in cooperation with the International Standards Organization developed such standards as V.90 for 56-kbps modems and X.25 for packet switching.

Furthermore, it has made a set of rules for the Clark orbit for geostationary communications satellites.

(visited February 2005). The definitive regulations can be found either in the ITU Radio Regulations or in Part 47 of the United States Code of Federal Regulations.

[48] Establish internationally agreed technical and operating standards “Recommendations” for networks and services.

[49] Assistance to developing countries to facilitate connectivity and access, foster policy, regulatory and network readiness, expand human capacity through training programs, formulate financing strategies and e-enable enterprises in developing countries.

[50] *ITU and its Activities Related to Internet-Protocol (IP) Networks* (Version 1.1, April 2004) at <http://www.itu.int/osg/spu/ip/itu-and-activities-related-to-ip-networks-version-1.pdf> (visited March 2006).

1.7.2. International Standards Organization

One of the most important international standards-setting and regulatory organizations is the International Standards Organization (ISO),[51] which covers areas of telecommunications and other areas. It is a non-governmental organization outside the United Nations system, but is a network of the national standards institutes of 156 countries. In particular, its Technical Committee 97 sets standards for data processing and data communications. Central to this effort is the ISO's Reference Model for Open Systems Interconnection (the OSI model), which defines a hierarchical structure within which open standards can be defined and defines seven "layers" of data handling during transmission. In the OSI model – which has been developed together with ITU - the lower level functions (those that are independent of the particular task in which the end users are engaged) are referred to as network functions. The higher-level activities (those that use the network functions to perform specific tasks) are called the end-to-end, or end-user, functions.

Some of the more notable standards developed within the OSI architecture is:

- X.400: The Message-Handling (E-Mail) System - a set of standards, functioning at the upper layers of the OSI model, for interoperability among electronic messaging services. X.400 divides e-mail networks into user agents and message transfer agents.
- X.500: The Directory Standard that is protocols to support a global directory of telecommunications users.
- X.25: The Packet-Switching Standard, which defines the interface with the packet data network at the network, data link, and physical layers.

1.7.3. Internet Engineering Task Force

The Internet Engineering Task Force (IETF) establishes operational standards for the Internet, such as continuing development of the Transmission Control

[51] <www.iso.org>.

Protocol/Internet Protocol (TCP/IP).[52] One of the continuing problems is the coordination of activities and standards of the IETF and the ITU. The IETF is the protocol engineering and development arm of the Internet. Though it existed informally for some time, the group was formally established by the Internet Architecture Board (IAB) as part of the nonprofit nongovernmental international Internet Society (ISOC)[53] in 1992. The IAB is responsible for defining the overall architecture of the Internet, providing guidance and broad direction to the IETF. The IAB oversees a number of critical activities in support of the Internet and also serves as the technology advisory group to the Internet Society. The latter is a professional membership organization of Internet experts that comments on policies and practices and oversees a number of other boards and task forces dealing with network policy issues.

1.7.4. Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is a private corporation registered in California and thus under the Law of California. It has with the United States Department of Commerce entered into an agreement or a "Memorandum of Understanding," originally entered into by the parties on 25 November 1998.

One primary task has been to fulfill the obligation of the Internet Assigned Numbers Authority (IANA), which is in charge of all "unique parameters" on the Internet, including IP (Internet Protocol) addresses. Each domain name is associated with a unique IP address, a numerical name consisting of four blocks of up to three digits each, e.g. 204.146.46.8, which systems use to direct information through the network.

1.7.5. International Telecommunications Satellite Organization

The International Telecommunications Satellite Organization (ITSO[54]) that

[52] Transport Control Protocol/Internet Protocol (TCP/IP) is a packet-switching protocol developed by the U.S. Department of Defense. It drives the system of interacted packet networks known as the Internet.

[53] <www.isoc.org>. See further this book Chapter 2, section 2.2.2.

[54] <http://www.itso.int>.

was called INTELSAT[55] until 18 July 2001 where the organization was restructured and created a commercial and pro-competitive company named "Intelsat Ltd."[56] has the following mission and main principles:

- Act as the supervisory authority of Intelsat, Ltd.
- Ensure the performance of core principles for the provision of international public telecommunications services, with high reliability and quality.
- Promote international public telecommunications services to meet the needs of the information and communication society.
- Maintaining global connectivity and global coverage for any country or territory that desires to connect with any other country or territory within and between the five regions of America, Western Europe, Eastern Europe, Africa and Asia.
- Providing public telecommunications services, including capacity and price protection guarantees, to customers identified as, and connecting with, "Lifeline Connectivity Obligation" ("LCO") customers.
- Providing domestic public telecommunications services between areas separated by geographic areas not under the jurisdiction of the State concerned, between areas separated by the high seas, or between areas that are not linked by any terrestrial facilities and which are separated by natural barriers of such an exceptional nature that they impede the establishment of terrestrial facilities; and
- Ensuring non-discriminatory access to Intelsat, Ltd.'s communications system.

ITSO's governing body is the "Assembly of Parties" that meets normally every two years. It has a executive organ headed by a Director General, which supervises and monitors Intelsat, Ltd's provision of public telecommunications services. ITSO is a multinational consortium of countries and their telecommunications providers. Membership is open to any country that

[55] U.S. Congress allowed by the Orbit Act of 2000 (Public Law 106-180 that amended the Communications Satellite Act of 1962) INTELSAT to be privatized.

[56] The company is based in Washington, DC and headquartered in Bermuda. The corporate structure of Intelsat, Ltd. includes several subsidiaries established under the laws of various countries, <www.intelsat.com>.

is a member of the ITU, but non-members may also use the space segment. As of March 2005, 148 nations were members of ITSO.[57]

Intelsat, Ltd. owns and operates 30 satellites and today offers a variety of telecommunications services. There are over 300 authorized users of the Intelsat-system, who may communicate over more than 27,000 Earth stations worldwide. The ITSO has jurisdiction over the space segment only. It does not construct, finance, or maintain the Earth stations needed to communicate with the system. But any application for a new Earth station that will use the system must be approved by ITSO. Approximately two-thirds of the world's international telecommunications traffic is carried by Intelsat Ltd. It is the only satellite system with nondiscrimination and universal service obligations.

There exists two main documents: the Agreement (the Intergovernmental Interim Agreement),[58] and the Operating Agreement (the Special Agreement).[59] The Agreement contains a clause permitting the organization to authorize other satellite systems separate from INTELSAT (so-called "Separate Satellite Systems").

1.8. Discussion

One basic requirement for a body that should govern the Internet must be that it is an international entity. This excludes any kind of an entity in shape of a corporation, which need to be incorporated in a State and thus follow that State's laws that might be or might not be in accordance with public international law.

[57] <http://216.119.123.56/dyn4000/dyn/docs/ITSO/tpl1_itso.cfm?location=&id=1&link_src=HPL&lang=english> (visited March 2005).

[58] Agreement Relating to the International Telecommunications Satellite Organization "INTELSAT", done at Washington August 20, 1971 (into force February 12, 1973) with annexes and Operating Agreement at <http://www.islandone.org/Treaties/BH585.html> (visited July 2006).

[59] Operation Agreement Relating to the International Telecommunications Satellite Organization "INTELSAT", done at Washington August 20, 1971 (into force February 12, 1973).

As ICANN is a corporation[60] and partly ITSO is a private commercial entity as Intelsat Ltd. is incorporated in the US neither of these organizations is suited to govern the public international networks.

The ISO is a truly international entity and thus not bound by a specific State's law wherefore it might be a possible governing organ for the Internet. Furthermore, it has as its purpose to make standards on telecommunications. However, it also makes standards for a variety of other areas other than telecommunication. As the entity that should govern the Internet ought to concentrate only on the Internet and not to be dealing with anything else, ISO as an international standardization entity should not be handed over the governance of the public international computer networks.

As the entity that should govern the Internet ought to concentrate only on the Internet and not to be dealing with anything else, ITU does neither seem to be suited to govern the Internet. Broadcast and phone-communication will probably for a long time require special national legislation, which latter should not be an issue for the public international networks. Specially the scarcity of the radio spectrum necessary for broadcasting imply that ITU's present tasks will never end and thus prevent ITU from ever being able to fully concentrate instead on public international computer networks. In addition, the ITU Member States has previously unanimously agreed that ITU should not take over ICANN's functions, which latter only deals with a part of what should be handed over to an Internet governance entity. Furthermore, the ITU is only a policy organization and has no enforcement powers, which an Internet governance entity must have.

The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. As such it does not have the organizational structure that is needed for an international organization governing the international networks of computers as its structure is to loose. Furthermore, it is open to any interested individual.

[60] *McNiel v Verisign & ICANN*, 2005 WL 741939 (9th Cir., April 2005)(Affirmed that plaintiff could not assert a First Amendment claim against ICANN because ICANN, a non-profit public benefit corporation established by agencies of the United States government to administer the Internet domain name system, is not a government actor).

This brings me to the conclusion that a completely new international entity is necessary. The "Constitution" for such an organization should be similar to the WSIS's Declaration of Principles for Internet Governance. Furthermore, the entity should be under the umbrella of the United Nations so it would have an obligation to respond to declarations from the U.N. Assembly and the still evolving public international law on human rights, including freedom of speech.

Furthermore, such a special public international entity would not have to take into consideration old times regimes on telecommunications and thus not deal with the convergence problems the Internet has caused.

Very essential for such a new entity is, that it is given some enforcement tools, for example allowing it to recall domain names used by a cybernaut in violation with international public law, and having Standing before the International Court of Justice against States that have violated international public law. Many other enforcement tools could be appropriate.

1.9. Violations

In connection with a discussion of public international law and governance of the Internet, it might be appropriate to look at some violations of public international law that have occurred in the past by States. Such violation should be an incitement for a future Internet governing entity to issue rules.

The same entity should also be aware of the fact that the computer has strained the familiar rules and categories in many areas of State's substantive law.[61] The use of telephone lines to carry data among computes has presented novel problems of telecommunications regulation. States have enacted elaborate rules to ensure that providers of computer communications obtain access to the telephone network on reasonable terms and conditions.

The Internet and its use to carry voice telephone calls and audio programming have created uncertainty as to the appropriate model for regulation of this new medium. The availability of computers has challenged family beliefs

[61] HARVEY L. ZUCKMAN, ROBERT L. CRON-REVERE, ROBERT M. FREDEN, CHARLES H. KENNEDY, MODERN COMMUNICATIONS LAW 775 (Hornbook Series – Student Edition, West Group, 1999 – ISBN 0-314-21176-4).

about the protection of informational privacy, for example whether the present patchwork of laws affecting access to databases, interception of electronic communications and the right of individuals to control the collection, accuracy and use of private information about themselves is adequate in the face of the explosion of data-gathering technology.

Some States have tried to govern the Internet with use of filters. If the filtering interfere with more than that states' own residents, public international law will be violated. If a State tries to stop packets from certain foreign states, the telecommunication will not be stopped, but will be rerouted. However, the efficiency of the Internet will be decreased as that State's notes will not work as cooperative as notes in "free" States, wherefore communication in "free States" will be tampered with.

A similar issue is raised by the argument of the government of the United States that it is allowed to conduct surveillance of nearly 70 % of the Internet traffic, as circa 70 % of the routing Internet servers are located in the U.S. The U.S.'s Patriot Act[62] – and national security – allows such surveillance. As national security concerns under public international law allow a State to intervene, the U.S. thus claims it has the right to oversee nearly all Internet telecommunication. However, this rule in public international law is a rule for exceptions.

Another type of violation of public international law has been the decision of a French court[63] to decide what content Americans should be allowed to put on websites. Yahoo in California has been given a court order to remove

[62] Especially 18 U.S.C. § 2510 - 2511 ("Interception of Computer Trespasser Communications") of USA Patriot Act of 2001 ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001"), Pub. L. No. 107-56 (Oct. 26, 2001).

[63] Two decisions of May 22nd 2000 and November 20th 2000 in *L'Association Union des Etudiants Juifs de France & La Ligue Contre Le Racisme et L'Antisémitisme v. La Société Yahoo! Inc. & La Société Yahoo France* (Tribunal de Grande Instance de Paris, No. RG 00/05308 & 00/05309) at <www.cdt.org-speech-001120yahoofrance.pdf> & as part of the Complaint in the American case at <http://www.cdt.org/speech/international/ 001221yahoocomplaint.pdf> (visited August 7 2001). Unofficial translations of the French orders can be found at <www.geocities.com/hssph/Order22May2000_EN_Toman.pdf> and <www.geocities.com/hssph/Order20Nov2000_EN_Toman.pdf>. See below Chapter 6.

certain content that has been uploaded by Americans on an American auction site and which content violate French law.[64] The French court has held it had jurisdiction over the Californian corporation, which does not do business in France. Such exercise of jurisdiction over the host of foreign website violates public international law on jurisdiction.

A similar jurisdiction violation is the English High Court's exercise of jurisdiction in *Schwarzenegger*[65] about an Internet libel suit launched against California Governor Arnold Schwarzenegger. The suit arose from an article in the American newspaper LA Times available online that discussed an alleged sexual harassment. The court held that an "Internet publication takes place in any jurisdiction where the relevant words are read or downloaded." Plaintiff was a Hollywood publicist that claimed the online publication happened in England and Wales, offering jurisdiction to an English court. Public international law has never allowed jurisdiction for a State that does not have a relevant connection with the claim. However, a rationale that foreign persons can read English and thus understand American websites and online newspapers should not be sufficient under international law for exercising jurisdiction.

Finally, it should be mentioned that section 4 of article 22 of the Cybercrime Convention[66] allows a foreign State through its law to criminalize offences done in Cyberspace of a cybernaut of another State even though the act is legal in the cybernaut's own State. This section in the convention may be a violation of public international law in form of for example human rights

[64] France law forbids sale of and exhibiting Nazi material, French Penal Code Article R645. Unofficial English translation at <www.geocities.com/hssph/R645-1_Toman.pdf>.

[65] *Anna Richardson v. Arnold Schwarzenegger, Sean Walsh and Sheryl Main* [2004] EWHC 2422 (High Court, Queens Bench Division, October 29 2004 – case no. HQ04X01371). See also, Case Comment: Arnold Schwarzenegger Case not Terminated, ENTERTAINMENT LAW REVIEW 2005, Ent. L.R. 2005, 16(6), 156-158.*Richardson v. Schwarzenegger*, [2004] EWHC 2422 (High Court, Queens Bench Division, October 29 2004).

[66] Convention on Cybercrime of 23 November 2001 (Council of Europe - ETS No. 185) - Into force July 1, 2004 - at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. See below Chapter 7 section 7.6.2.

instruments.

1.10. Final remarks

My suggestion is that the public international computer networks should be governed by a completely new entity established under the United Nation.[67] Such an entity should immediately make rules on issues, which previous have shown to be violation of states.

Another alternative to Internet governance would be to decide that the Internet is a "High Sea" and make a treaty that outlines the rules for the international public computer networks. However, the work of making a comparison between the different rules of U.N. Treaty on the High Sea and the Internet is a task far beyond this chapter. In this connection should be noted that the United Nations already has passed a resolution declaring that "communications by means of satellite should be available to the nations of the world as soon as practical, on a global and nondiscriminatory basis," which statement already is a basis for ITSO (previous called INTELSAT).[68]

The U.S.'s behavior[69] related to the Internet's DNS-system[70] seems like

[67] This view is also argued for in UNESCO's series on Law of Cyberspace series, THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 142 (UNESCO Publishing, 2000 – ISBN 92-3-103752-8).

[68] UN General Assembly, 16th Session, resolution 1721, section D of 20 December 1961 on International Co-operation in the Peaceful uses of Outer Space, at <http://daccessdds.un.org/doc/RESOLUTION/GEN/NR0/167/74/IMG/NR016774.pdf ?OpenElement>.

[69] "We want to strongly reiterate our support for continued Department of Commerce control over the so-called "A-root" server. We believe that any assumption of control over that asset by any outside entity would be contrary to the economic and national security interests of the United States," from letter of 13 March 2002 from Representatives in the U.S. Congress to Secretary of U.S. Department of Commerce at <http://www.icannwatch.org/article.pl?sid=02/03/14/122633> (visited March 2005). There exist 13 root-servers in the world and these are maintained by different organizations, see further Root Servers Technical Operation Association at <www.root-servers.org>.

[70] Domain Name System is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The DNS system is in itself a network. If one DNS server does not know how to translate a par-

the behavior of previous colonial-powers in the last century. As the Internet crosses national borders, individual governments cannot properly manage the domain name system.[71] The U.S. Government has not been willing to "surrender the control over it to the global community."[72] It is an old fashion and non-democratic way of behavior that is unacceptable for the rest of the International Society in the twenty-first century. The Internet was far from build by American-born scientist alone – and for certain, the worldwide used www-application, http, developed outside the U.S., was the one that made the use of the Net customer friendly and made its use explode – also in the U.S.[73] Some countries, including the E.U., has offered to make and facilitate an (easy made) alternative on behalf of the whole world,[74] and it will be easy technically for the world outside to outsource U.S. root-servers if the U.S. wants to behave as an isolationist (or attempts to be a "IT-superpower". However, the U.S. seems at the latest to have changed its position.[75]

Until a truly international body has been established, leaders of govern-

ticular domain name, it asks another one, and so on, until the correct IP address is returned.

[71] *The Domain Name System: A case study of the significance of norms to Internet Governance*, Harvard Law Faculty, HARVARD LAW REVIEW, 112 HVLR 1657, 1658 (1999).

[72] *U.S. Principles on the Internet's Domain Name and Addressing System* at <www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm> (visited July 5, 2005).

[73] Berners-Lee, the chief architect of the World Wide Web, has stated that the "whole point of the Web is when you arrive it's more or less the same for everybody. That integrity is really essential. I'm very concerned" if for example broadband providers abandoned the principle of Net neutrality, Tyler Hamilton, *Battle for the Web*, TORONTO STAR, March 28, 2006 at <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1143499812060&call_pageid=968350072197&StarSource=RSS> (visited March 28, 2006).

[74] Tom Wright, *EU Tries to Unblock Internet Impasse*, THE NEW YORK TIMES, September 30, 2005 at <www.nytimes.com/iht/2005/09/30/business/IHT-30net.html> (visited October 14, 2005).

[75] Victoria Shannon, *A Compromise of Sorts on Internet Control*, THE NEW YORK TIMES, November 16, 2005 at <www.nytimes.com/2005/11/16/technology/16net.html> (visited 16 November 2005).

ments, organizations and private parties involved in Internet telecommunication should keep in mind the content of the Declaration of Principles for Internet Governance from the U.N. World Summit on the Information Society (WSIS).[76] Those principles would at least prevent some of the violations of public international law that have occurred, and serve as guidance for future conflicts related to public international computer networks.

[76] Build to a large extent on the U.N. Declaration on Human Rights, adopted by UN General Assembly Resolution 217A (III) of 10 December 1948 and the Article 19 of International Covenant on Civil and Political Rights, Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976, U.N.T.S. No. 14668, vol. 999 (1976), p. 171.

CHAPTER 2

IPv6 – Possibilities of Dividing Cyber-space into Jurisdictions

By Henrik Spang-Hanssen[1]

2.1. Introduction

This chapter will deal with the Internet Protocol (hereinafter IP) and make a survey of how the present version IPv4 works, especially what kind of limits there are available for Nations to hinder data to pass that Nation's telecommunications pipe lines. Furthermore, make a survey of the differences between IPv4 and the next generation, IPv6 or IPng, especially as to whether the new version allows Nations to hinder data to its citizens.

The Internet is not an application but a data delivery service. "Data" is not in itself a service: it is a way of sending the information contained in an application. To a telecommunications transmission technology, a signal may be a stream of bits, but to a user it is a telephone call, a webpage, music program, or a television program. Thus, data may be carried over terrestrial or satellite-based telephone networks, over public or private terrestrial data networks, or over satellites.[2]

[1] I'll like to thank Professor and Director of the Broadband Institute of California Allen Hammond, High Tech Law Institute, and professor Hans-Peter Dommel, School of Computer Engineering, for comments to this chapter.

[2] MARK R. CHARTRAND, SATELLITE COMMUNICATIONS FOR THE NONSPECIALIST 345-47 (Spie Press 2004 – ISBN 0-8194-5185-1) [hereinafter CHARTRAND]. Article 1(d) of the Cybercrime Convention defines "traffic data" as "means any computer data relating to

In the last decades, networks based on the Internet Protocol have become the norm. Support for both voice and data services over IP gave rise to the term "converged networks", which can support both real-time (voice and video) and non-real-time (data) applications.

A protocol is a standard in an open system of computer networks, see further section 2.2.3. The IP protocol is a protocol for Internet routing[3] at the Network Layer or Internet Layer, see further section 2.3. It is closely connected to another vital protocol for the functionality of the modern networks, the Transmission Control Protocol (hereinafter TCP) from 1973, which is for reliable[4] end-to-end transport. It is a protocol at the Transport Layer or Host-to-Host[5] (Service) Layer. It acts as a buffer between the Communications Subnet (Physical, Data Link and Network layers) and the Host Process (Session, Presentation and Applications layers),[6] see table 2.6 below.

The TCP/IP protocol suite consists of a large collection of protocols that have been issued as Internet standards by the Internet Architecture Board (IAB), see further section 2.2.2.

At this time should be pointed out, that the term "datagram"[7] refers to a

a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"; and "computer data" as "means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function," article 1(b)., "Budapest Convention" of 23 November 2001 at <www.coe.int/T/E/communication_and_Research/Press/Themes_Files/Cybercrime> or <http:://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>.

[3] See further chapter 5 of T. Socolofsky & C. Kale, *A TCP/IP Tutorial*, RFC 1180 (Jan. 1991).

[4] UDP (User Datagram Protocol) is for applications that don't need reliable delivery and is more efficient to be used on top of IP.

[5] Any node that is not a router. The latter is a node that forwards IP packets (= datagrams) not explicitly addressed to itself.

[6] MARK A. MILLER, INTERNET TECHNOLOGIES HANDBOOK 22-24 & 31 (Wiley-Interscience, 2004 – ISBN 0-471-48050-9) [hereinafter MILLER].

[7] An IP datagram is the unit of end-to-end transmission in the IP protocol. It consists of an IP header followed by transport layer date, R. Braden (ed.), *Requirements for Internet Hosts – Communication Layers* page 17, RFC 1122 (Oct 1989). The maximum size

package of data transmitted over a connectionless network. "Connectionless" means that no connection between source and desolation is established prior to data transmission. Datagram transmission is analogous to mailing a letter. With both a letter and a datagram, one write source and destination addresses on the envelope place, the information inside, and drop the package into a mailbox for pickup, But while the post office uses blue or red mailboxes, the Internet uses ones network node as the pickup point.[8]

2.2. Public International Computer Network

A major contributor to the Internet's success is the fact that there is no single, centralized point of control or promulgator of policy for the entire network. This allows individual constituents of the network to tailor their own networks, environments and policies to suit their own needs. The individual constituents must cooperate only to the degree necessary to ensure that they interoperate.[9]

2.2.1. Public International Law

The Internet is a web of networks of computers around the world. A Working Group under the International Telecommunications Union (ITU) has defined the Internet as the publicly accessible global packet switched network of networks that are interconnected through the use of the common network protocol IP.[10] It encompasses protocols; names and addresses; facilities; ar-

datagram that all hosts are required to accept or reassemble from fragments is 576 octets, J. Postel, *The TCP Maximum Segment Size and Related Topics* page 1, RFC 879 (Nov 1983).

[8] MILLER, *supra* note 6 at 64.

[9] F. Kastenholz and C. Partridge, *Technical Criteria for Choosing IP: The Next Generation*, RFC 1726 (December 1994).

[10] H. Zhao, *ITU and Internet governance*, 15 December 2004, ITU Council Working Group on the World Summit on the Information Society Geneva 13-14 December 2004, WG-WSIS-7/6 Rev 1 at <www.wgig.org/working-papers.html> (visited March 2005).

rangements; and services and applications.[11]

It does not belong to any State or group of States in the world. Thus, the Internet is something like the High Sea belonging to the international society of States and under the reign of public international law.

This public international law is the sum total of legal norms governing rights and duties of the collectivities of the ruling classes - civilized participants in international intercourse in war and peace[12] - without which it would be virtually impossible for the participants to have steady and frequent intercourse.[13] It is not rules, but a normative system that operates in a horizontal legal order.[14] Public international law is a process, a system of authoritative decision-making.[15] It deals with the conduct of nation-states and their relations with other states, and to some extent also with their relations with individuals, business organizations, and other legal entities. In its conceptions, its specific norms and standards, and largely in practice, international law functions between states, as represented by their governments.

International public law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims.[16] There is no central legislature with general

[11] On ITU's packet-switching standard X.25, see CHARLES H. KENNEDY, AN INTRODUCTION TO INTERNATIONAL TELECOMMUNICATION LAW 40-46 (Artech Houce Inc, 1996 – ISBN 0-890068356).

[12] HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION - POSSIBILITIES OF DIVIDING CYBERSPACE INTO JURISDICTIONS WITH HELP OF FILTERS AND FIREWALL SOFTWARE 300 (DJØF Publishing, Copenhagen, 2004 - ISBN 87-574-0890-1) [hereinafter SPANG-HANSSEN].

[13] I.A. SHEARER, STARKE'S INTERNATIONAL LAW 14 (11th Edition, Butterworth).

[14] ROSALYN HIGGINS , PROBLEMS & PROCESS – INTERNATIONAL LAW AND HOW WE USE IT 1 (Clarendon Press, Oxford 1994 – ISBN 0-19-876410-3), Rosalyn Higgins , *International Law and the Avoidance, Containment and Resolution of Disputes – General Course on Public International Law*, RECUEIL DES COURS, Vol. 230 (1991-V) page 23.

[15] *Id*. PROBLEMS & PROCESS, at 267.

[16] Introduction note to Part I, Chapter 1 of Restatement (Third) of Foreign Relation Law [hereinafter REST-Foreign]. Restrictions upon the independence of States cannot

law-making authority and there is no executive institution to enforce law.

It is to be distinguished from Private International Law or Law of Conflicts, which cover a certain State's rules on judicial jurisdiction and competence, foreign judgments and choice of law.[17] It is law directed to resolving controversies between private persons, natural as well as juridical, primarily in domestic litigation, arising out of situations having a significant relationship to more than one state.

Increasingly, public international law impinges on private international activity, for example, the law of jurisdiction and judgments and the law protecting persons.[18]

There exist no treaties which require a freedom of speech combined with a right to crossborder telecommunication. However, there exist some international declarations that suggest such a regime, for example Article 19 of the Universal Declaration of Human Rights[19] and Article 19 of the International Covenant on Civil and Political Rights.[20] However, this does not mean under international law that free speech cannot be limited by a nation through legislation.

Thus, under international law nations are to a certain degree allowed to make limits in people's right to publish their opinions, especially if it is related to national security issues, or culture and religious issues, which are often mentioned in a nation's constitution

therefore be presumed. *S.S. Lotus* (France v. Turkey) 1927 P.C.I.J. (Ser. A) No. 10 para. 18. Also at <www.geocities.com/hssph/Lotus.doc>.

[17] Municipal law governs the domestic aspects of government and deals with issues between individuals, and between individuals and the administrative apparatus, MALCOLM N. SHAW, INTERNATIONAL LAW 82 & 100 (4th Edition, Cambridge University Press); IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW at chapter 2 (6th Edition, Clarendon Press, Oxford) [hereinafter BROWNLIE]. The International Court of Justice in the *Barcelona Traction, Light, and Power Co, Limited* (Belgium v. Spain) (Second Phase) of February 5, 1970, 1970 I.C.J. 3, referred to the rules generally accepted by municipal legal systems, not the municipal law of a particular state.

[18] Comments to § 101 of Restatement (Third) of Foreign Relations Law.

[19] Adopted by UN General Assembly Resolution 217A (III) of 10 December 1948.

[20] Adopted by U.N. General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976, U.N.T.S. No. 14668, vol. 999 (1976), p. 171.

On the other hand as for free speech and international public law, there exists no international law stating a nation's citizen has to cut off content that is legal in at least one foreign nation besides the citizens own nation - and thus probably acceptable to the U.N. Declaration of Human Rights on free speech.

Thus, under public international law most Internet-telecommunication are not under any control of any fortuitous State as in practice most of the information on the Internet is placed on serves outside the State in question.

At this place should be mentioned that satellites as for the cobber-lines only are part of the "pipe" lines for the international public networks and that a State is not allowed to hinder or interfere data-delivery designated between two foreign States by passing another State's territory including airspace.

A State under public international law has the right to make legislation over or totally forbid Earth stations in its territory to communicate with satellites. Under international law the territory include the air space above, but there is no definite km-limit. On the other hand, public international law does not allow a State to legislate or make enforcement on satellites and the telecommunication that is offered by a certain satellite if the satellite is not in a to narrow distance from the Earth.[21] (It should be noted, the State in which the owner of a satellite is located or incorporated of cause can give binding orders to that owner). Except for satellites in the Clarke Orbit,[22] which is govern internationally by the ITU,[23] anyone can launce a satellite into orbit and offer telecommunication including the information that can be achieved from the international computer networks.

[21] BROWNLIE *supra* note 17, at 105, 255-259, OPPENHEIM 'S INTERNATIONAL LAW 479, 650, 662, 826-845 (London and New York: Longman 9th Ed., paperback edition 1996))[hereinafter OPPENHEIM], and D.J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 244 (5th Edition, Sweet & Maxwell, ISBN 0-421-53470-2Hb).

[22] Or the Geosynchronous Orbit. Satellites in this orbit (GSOs) are launched into a band 35,786 (22,300 miles) in altitude above Equator where it moves in consonance with the terrestrial globe and therefore is constantly over the same point. Three GSO-satellites can cover the total surface of the Earth. However, a GSO satellite cannot see any areas with latitude more than 77° north or south.

[23] Because the Clarke Orbit is only of 265,000 km in range is requires an administration of this "limited natural resource" like the radio frequencies also administrated by ITU.

Thus, under public international law most Internet-telecommunication are not under any control of any fortuitous State as in practice most of the information is only in "transit" through the "pipe-line" of that state in form of a bit send from a foreign country A to country B.

2.2.2. The Internet Society

The Internet as no other "organization" - avant-garde or not - cannot operate without some degree of structure. The nonprofit nongovernmental international Internet Society (ISOC),[24] which was founded in 1992 with headquarter in Virginia for global cooperation and coordination for the Internet, provides some of that structure. One of ISOC's components is the Internet Architecture Board (IAB),[25] chartered in 1992.
The IAB consists of 13 members: 12 full members plus the chair of the Internet Engineering Task Force (IETF).26 The IAB's responsibilities include:[27]

- Appointing a chair of the IETF and its subsidiary Internet Engineering Steering Group (IESG)
- Oversight of the architecture for the protocols and procedures used by the Internet
- Oversight of the process used to create Internet standards
- Editorial management and publication of the Request for Comment [hereinafter RFC[28]] document series and administration of the various Internet assigned numbers
- Representing the interests of the Internet Society to other organizations

[24] <http://www.isoc.org>.
[25] <www.iab.org>.
[26] The IETF IPv6 Working Group maintains a website with current information regarding IPv6 development and documentation activities at <http://www.ietf.org/html.charters/ipv6-charter.html> and S. Bradner, *The Internet Standards Process - Revision 3*, RFC 2026 (October 1996).
[27] B. Carpenter (Ed.), *Charter of the Internet Architecture Board*, RFC 2850 (May 2000).
[28] Request for Comments (RFC) website is <http://www.ietf.org/rfc.html> (visited October 2005). On the process, see R. Hovey, *The Organizations Involved in the IETF Standards Process*, RFC 2028 (October 1996) & RFC Editor et al., *30 Years of RFCs*, RFC 2555 (April 1999).

- Providing guidance to the Internet Society regarding Internet technologies

Two task forces report to the IAB. The IETF coordinates the technical aspects of the Internet and its protocols and ensures that it functions effectively. The Internet Research Task Force (IRTF) researches new technologies.

The IAB produces numerous protocol standards and operational procedures that require dissemination and archiving, mostly as RFCs.[29]

Two sources of information on Internet standards and parameters are updated on a periodic basis. The Internet Assigned Numbers Authority (IANA) documents protocol parameters, assigned addresses such as port numbers, and many others.[30] The Internet Official Protocol Standards document[31] describes the standards track process and lists recently published RFCs and the current standardization status of the various protocols.

The protocols of the Internet can be divided into three categories (for IP see RFC 791[32], for TCP see RFC 793[33] and for UDP see RFC 768)[34]:

a. Core Protocols
b. Control, routing, and Address Resolution Protocols
c. Multimedia Protocols

Virtually all computer vendors now provide support for this architecture.

2.2.3. The International Organization for Standardization

Besides the above mentioned so-called ARPA-system, another layer-concept of an Open Systems Interconnection (OSI) has been developed by the Inter-

[29] Some libertarian users see the practice of issuing a RFC as a source of "customary" cyberspace law, Elisabeth Longworth, *The Possibilities for a Legal Framework for Cyberspace, in* THE INTERNATIONAL DIMENSION OF CYBERSPACE LAW 30 (Law of Cyberspace Series Vol. 1, Ashgate Publishing 2000 – ISBN 0-7546-2146-4).

[30] IANA maintains an online database of protocol numbers and parameters at <www.iana.org/numbers.html>.

[31] Currently document is J. Reynolds et. al., *Internet Official Protocol Standards*, RFC 3300 (November 2002).

[32] Jon Postel, *Internet Protocol*, RFC 791 (1981).

[33] Information Sciences Institute, University of Southern California, *Transmission Control Protocol*, RFC 793 (September 1981).

[34] Jon Postel, *User Datagram Protocol*, RFC 768 (August 1980).

national Standards Organization (sometimes called "International Organization for Standardization") (ISO),[35]

This system has in stead of ARPAs 5 layers (see below Table 2.6) a seven-layer OSI Reference Model, which also allow various vendor-systems (or "open"-systems) to communicate.

However, its seven layers make it more complicated to use and the concept has not been as widely used as the ARPA. In the ISO's seven layers - in general terms - the lower five layers provide connectivity functions, while the upper two layers provide interoperability functions, see table 2.6. The first is comprised of the lower three layers (the Physical, Data Link, and Network Layers) and is termed the "communications subnetwork", "subnet", or the carrier portion of the system. The upper three layers (the Session, Presentation, and Application Layers) are collectively known as the "host process", sometimes called the "customer portion" of the system. The middle layer (Transport) is the first end-to-end layer, and acts as a buffer between the two subsets. As such, the Transport Layer is often grouped with the upper layers as part of the host process.

2.2.4. The Internet

The Internet was built on the demand that nobody should be able to hinder telecommunication[36] from end user A to end user B. It is a data delivery service. The TCP and IP (usually referred to as TCP/IP) define how the data is partitioned and carried into a packet switching system, and contain techniques for error control. TCP/IP is a connection-oriented protocol meaning that it relies on getting acknowledgments of each data packet sent out. The IP is a network layer protocol and its task is to deliver packets of data from a source host to a destination host.

The inventors of the IP protocol wanted to make a borderless and international public computer network where people could get access to information on foreign computers and thus exchange point of views. Thus, this computer

[35] Information Processing Systems – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1 (1994).

[36] "Telecommunication" means communication at a distance electrically or electronically, CHARTRAND, *supra* note 2 at 37.

network was not made to belong to any special State or group of nations, but was intended to belong to the whole world.

The evolution of the public networks has been as table 2.1 shows.[37]

Year	Event
1966	U.S. Defense Advanced Research Projects Agency (ARPA or DARPA) packet-switching experimentation
1969	First ARPANET nodes operational at Stanford Research Institute (SRI), University of California at Santa Barbara (UCSB), University of California at Los Angeles (UCLA) and University of Utah.
1972	Ray Tomlinson of Bolt Baranek and Newman (BBN) wrote the first package to provide distributed mail systems – e-mail.
1973	¾ of all ARPANET traffic is e-mail First non-U.S. computer linked to ARPANET[38]
1974	Vint Cerf and Bob Kahn of ARPA published paper on methods and protocols for internetworking (across arbitrary, multiple, packet-switched networks, for example tactical radio communications and satellite communications (SATNET))[39]
1975	ARPANET its transferred from ARPA to Defense Communications Agency
1980	TCP/IP experimentation begins with major contributions from partici-pants from European Networks.
1981	New host added every 20 days U.S. National Science Foundation (NSF) approve funding for the Computer Science Network (CSNET)
1983	TCP/IP switchover complete

[37] On history of the TCP/IP protocol, see interview with Internet Pioneer Vint Cerf at <http://www.ibiblio.org/pioneers/cerf.html> (visited April 2003).

[38] *History - ARPAnet 1957 – 1990*, at <http://www.jmusheneaux.com/21bb.htm> (visited December 21, 2005); A Note on the Internet page 2, Graduate School of Business, Stanford University 1996, at <www.stanford.edu/group/scip/Afeche-internet.pdf> (vis-ited December 21, 2005).

[39] Vinton G. Cerf & Robert E Kahn, *A Protocol for Packet Network Intercommunication*, IEEE Transactions on Communications, May 1979, Vol. Com-22, Number 5 page 637, The IEEE COMMUNICATIONS SOCIETY [hereinafter KAHN].

1984	ARPANET split into two different networks: MILNET (for unclassified military traffic) and ARPANET (for nonmilitary traffic and research)
1986	NSF established the Office of Advanced Scientific Computing (OASC), which developed NSFNET with higher transmission rates and a new net backbone was created
1990	ARPANET shut down
1991	World Wide Web (www) invented by Tim Berners-Lee at the European Laboratory for Particle Systems (CERN) Pretty Good Privacy (PGP) released (technique developed by Philip Zimmerman for encrypting messages) Gopher introduced by University of Minnesota (A system that predates the World Wide Web for organizing and displaying files on internet servers) Commercial Information Interchange (CIX) formed by General Atomics, Performance Systems International and UUNNET Technologies to interchange traffic without no extra charge
1992	The first graphically oriented browser (Mosaic) introduced The international non-profit Internet Society (ISOC) founded
1993	NSF stopped traditional backbone architecture and instead specified a number of locations – Network Access Points (NAPs) – where various ISPs could inter connect and exchange traffic. 1 million users of the Internet [40]
1994	The London Internet Exchange (LINX) formed
1995	Internet backbone privatized by U.S. government. NSFnet shut down and replaced by the very high-speed Backbone Network Service (vBNS).
1996	CIX has become a 147 member network LINX has become a 24 member network
1997	60 million users of the Internet in 160 countries in the world [5]
1998	Over 2 million registered domain names
2000	Over 1 billion indexable web pages

[40] SPANG-HANSSEN *supra* note 12, page 535.

2005	By the end of 2005 China had 111 million Net users. Every fifth Chinese had a mobile phone, in total 383 millions. In the last quarter of 2005, 46.8 % of all spam came from the U.S. and China (nearly equally).

Table 2.1: Internet Evolutions.[41]

The first computer network was involving servers placed in United States, Norway and England.[42] Thus, the computer network from the very beginning has been an international network. The development of the public networks has been as table 2.2 indicates.

Year	Networks
1971	3
1980	20
1983	60
1985	300
1986	500
1990	900
1993	19,000
1996	50,000

Table 2.2: Operational Networks on the Internet.[43]

[41] Partly from WILLIAM STALLINGS, HIGH-SPEED NETWORKS AND INTERNETS: PERFORMANCE AND QUALITY OF SERVICE 5 (2. ed. 2002, Prentice Hall – ISBN 0-13-032221-0) [hereinafter STALLINGS-1] and MILLER, *supra* note 6 at Chapter 1.

[42] *History - ARPAnet 1957 – 1990*, at <http://www.jmusheneaux.com/21bb.htm> (visited December 21, 2005); *A Note on the Internet* page 2, Graduate School of Business, Stanford University 1996, at <www.stanford.edu/group/scip/Afeche-internet.pdf> (visited December 21, 2005).

[43] MILLER *supra* note 6, at 4.

2.3. Technique in the Public International Computer Network

Technically the Internet is analogous to an international system of roads and highways, where the national borders only are like street bumps. Its backbone - the superhighways of the Internet - carries large amounts of information over long distances and there are interchanges on the backbone at network access points (NAP's) and metropolitan area exchanges (MAE's). The "regional" highways is provided by large Internet Service Providers (ISP's) and "local ISP's provide "local streets" to the single user's computer or a company's network (a Intranet[44]).[45]

A system that complies with standards - also referred to as "protocols" - for communication with other systems is defined as being "open".

Communication is achieved by having the corresponding, or "peer", layers in two systems communicate. The peer layers communicate by means of formatted blocks of data that obey a set of rules or conventions known as a protocol. The key features of a protocol are as follows:[46]

- Syntax: Concerns the format of the data blocks
- Semantics: Includes control information for coordination and error handling
- Timing: Includes speed matching and sequencing

[44] Intranet – a private network, within a company or organization, that serves shared applications intended for internal use only – although some may be found on the public Internet.

[45] To speed that communication process, some telecommunications providers have agreed upon connecting and sharing – so-called "peering" – their respective fiber-optic channel-networks without charge - the network equivalent of a high-speed-freeway. However, these ISPs might not always cooperate. E.g. in December 2002 AOL shout out the U.S. high-speed Internet Access provider Cogent's network from using AOL's network, because Cogent caused AOL's network to carry more than twice the traffic back to its users as it sent to other users outside its network. This implemented that Cogent's users' – including George Town University in Washington D.C. - communications-speed was slowed down remarkably as AOL's network is huge in the U.S. Yuki Noguchi, WASHINGTONPOST.COM, December 28, 2002, at <http://www.washingtonpost.com/wp-dyn/articles/A45819-2002Dec27.html> (visited January 7 2003).

[46] STALLINGS-1 *supra* note 41, at 28.

The IP provides multiple routes from one point or "node"[47] to another with an automatic system, which simply reroutes communication if one part has heavy traffic or is damaged.

Every communication is broken into packets by the TCP, so each packet contains the addresses of the sending and receiving computers along with the information to be communicated.

The IP is responsible for routing the packets to their destination. Each packet may take a different route across the Internet - and packets may be broken up into fragments. Routers look at the destination address and forward the packet to the next router based on IP addresses and routing tables.[48] The IP does not guarantee the delivery of every packet.[49]

On the destination computer, TCP joins the packets into the complete communication and may have to reassemble fragmented packets. TCP may have to request retransmission of missing packets.[50]

Web browsers and Web servers communicate using the TCP/IP. The Web browser sends a request to the Web server, which request includes a portion of the URL for the requested Web page and the version of the HTTP protocol being used. The Web server responds to the request by sending the contents of the requested Web page to the computer on which the Web browser resides.[51]

[47] A device that implements IPv4 or IPv6.

[48] A node that forwards IP packets (= datagrams) not explicitly addressed to itself. Routers and switches are critical network infrastructure components by being key devices in controlling network traffic and linking together computer networks at greater scale. Switches interlink physical segments of a network and allow date to be exchanged between these segments. Switches can be compared to a train station or airport dynamically interconnecting different travel pathways, Hans-Peter Dommel, *Routers and Switches*, in HANDBOOK OF INFORMATION SECURITY (Hossein Bidgoli Ed., 2006, Wiley – ISBN0-471-64833-7).

[49] An every 5 minute updated Internet Traffic Rapport can be found at <http://www.internettrafficreport.com/main.htm> which shows the average packet loss on serves on different continents (visited 14 October 2003).

[50] See RFC 793 *supra* note 33 and RFC 1122 *supra* note 7.

[51] Thus, when a user in his browser ask to get and see a certain website, then the user via the IP protocol send a request to the web-server, that then send the webpage by packets in the IP protocol to the user's machine where the webpage is reassembled. It should be pointed out that parts of the webpage can come from different (proxy-) servers.

Initially, the Web browser establishes a connection with a Web server through a network before it can obtain the file from the Web server. Typically, this connection is established on the Internet via the TCP/IP connection. To establish a TCP/IP connection, the transport-layer protocol software initiates a request to connect to a special protocol port[52] of the Web server. If the address of the Web server is specified as an IP address in the URL for the requested page, then the computer running the Web browser initiates a request to resolve the domain name into an IP machine address name. Once the TCP connection is made, the Web browser can send repeated Web page requests to the same server without making a new connection.

Under the current Internet Protocol system, each machine connected to an Internet Protocol network is addressed using a unique IP address. These addresses are written in "dotted quad" notation, as a series of four 8-bit numbers, written in decimal and separated by periods, each ranging from zero to 255. When working with groups of computers (local networks) they are usually identified as the group with a base IP address, where the individual computers then are identified by a so-called "Subnet Masks", which by its last part identify the specific computer on the local network. Subnet masks are always used in conjunction with base IP addresses. A URL is a numeric Internet Protocol or "IP" address, and for convenience, most Web servers have alphanumeric "domain name" addresses in addition to IP addresses.

Many machines have more than one IP address. For example, a machine hosting multiple websites often has an IP address for each website it hosts. Other times, a pool of IP addresses is shared between a number of machines, e.g. on a dynamic IP dialup connection such as "Prodigy" – a Internet Service Provider - a subscriber's machine will be allocated a different IP address each time the subscriber connects.

In general terms, communications can be said to involve three agents: applications, computers, and networks.

A specific Internetwork architecture results when two open systems are linked directly with a bi-directional communication channel such as a cable.

[52] The port is simply a designator of one of multiple message streams associated with a process. A port address designates a full duplex message stream, KAHN supra note 39, at 637, 641.

The interface between the layers within the same system is a vertical relationship, whereas the protocol is a horizontal relationship between peer layers of the adjacent systems.

Packets are construed in such a way that layers for each protocol used for a particular connection are wrapped around the packet. At each layer - except at the application layer - a packet has two parts:

- Header – protocol information relevant to that layer
- Body – contains the data for that layer, which often consists of a whole packet from the next layer in the stack.

Each layer treats the information it gets from the layer above it as data, and applies its own header to this data. At each layer, the packet contains all of the information passed from the higher layer; nothing is lost. The process of preserving the date while attaching a new header is known as encapsulation.

At the other side of the connection, this process is reversed – header is striped at each layer. In trying to understand the packet filtering, the most important information is the headers of the various layers.

Table 2.3, 2.4 and 2.5 show the TCP and IP header formats.

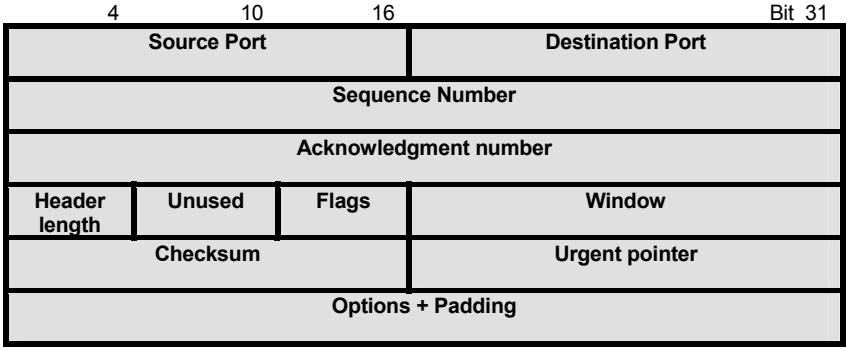

Table 2.3: TCP Header (20 octets and 32 bit)

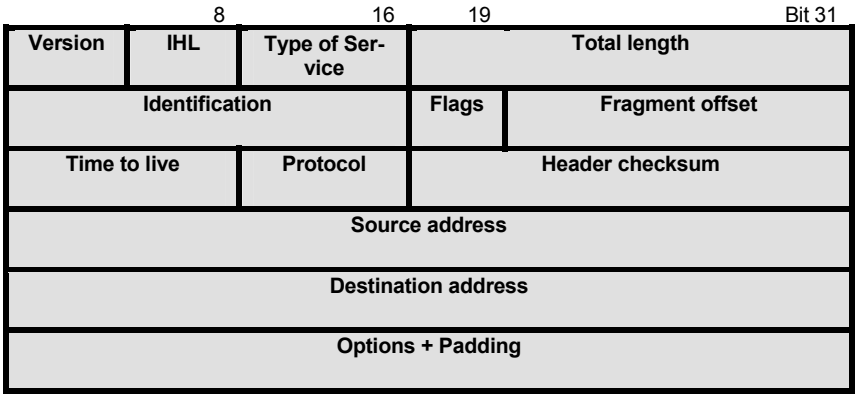

Table 2.4: IPv4 Header (20 octets and 32 bits)

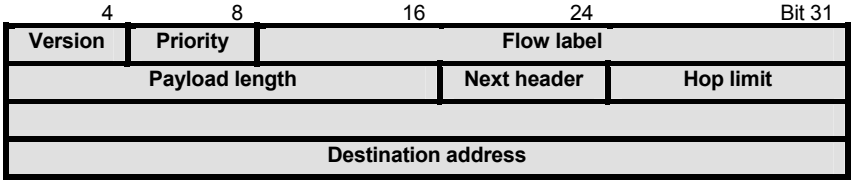

Table 2.5: IPv6 Header (40 octets and 31 bit)

Both the IP header and the TCP header may vary in length. Each network has some maximum packet size, and gateways[53] must be prepared to fragment datagrams to fit into the packets of the next network. The default rule is: "If the TCP Maximum Segment[54] Size is not transmitted then the data sender is allowed to send IP datagrams of maximum size (576) with a minimum IP

[53] Gateway - The point of contact between two wide-area networks. On the World Wide Web, a facility for adding scripts to handle user input. It allows a Web server to communicate with other programs running on the same server in order to process data input by visitors to the Web site.

[54] Segment is the unit of end-to-end transmission in the TCP protocol. It consists of a TCP header followed by application data and is transmitted by encapsulation inside an IP datagram, RFC 1122 *supra* note 7, at 16.

header (20) and a minimum TCP header (20) and thereby be able to stuff 536 octets of data into each TCP segment."[55]

Packet filtering systems route packets between internal and external hosts selectively. They allow or block certain types of packets according to a security policy.

At the Application Layer (see Table 2.6), the packet consists simply of the data to be transferred. As it moves to the transport layer, the TCP or the User Datagram Protocol (UDP) preserves the data from the previous layer and attaches a header to it. At the next layer, the IP considers the entire packet (consisting now of the TCP or UDP header and the data) to be data and now attaches its own IP header. Finally, at the Network Layer Ethernet or another network protocol considers the entire IP packet passed to it to be data and attaches its own header, and sent the whole thing to the other node.

The Transport Layer – or Host-to-Host Layer (se Table 2.6) - has two primary protocols, TCP and the UDP. The latter is a connectionless protocol and is used by developers if is more important to develop a streamlined, low overhead application. The first is a connection-based protocol that provides error detection and correction with reliable delivery of data packets. The major difference between the Data Link and Transport Layers is that the Data Link domain lies between adjacent nodes, whereas the Transport Layer's domain extends from the source to the destination (or end-to-end) within the communication subnet. Issues concerning source-to-destination messages are important in the Transport Layer. For example, the Transport Layer segments a long message into smaller units (packets) prior to transmission, and assure the reassembly of those packets into the original message at the receiver's end.

In those cases where two devices are attached to different networks, procedures are needed to allow data to traverse multiple interconnected networks. This is the function of the Internet Layer – or the Network Layer. The Internet Protocol (IP) is the primary protocol at this layer of the TCP/IP architecture mode and is used at this layer to provide the routing function across multiple networks. This protocol is implemented not only in the end systems but also in routers. The Network Layer switches, routes, and controls the

[55] RFC 879 *supra* note 7, at 9.

congestion of these information packets within the subnet. Thus, the Internet Layer manages the connections across networks as information is passed from source to destination. The IP is a connectionless protocol and it does not itself provide error checking and correcting functions. Another protocol at this layer of the TCP/IP architecture model is the Internet Control Message Protocol (ICMP), which is used to communicate control messages between IP systems.[56]

[56] CHARLES H. KENNEDY AN INTRODUCTION TO INTERNATIONAL TELECOMMUNICATION LAW 38 (Artech Houce Inc, 1996 – ISBN 0-890068356).

		ARPA Layer	OSI Layer	Protocol Implementation							
Host Process	Interoperability Function	Process / Application	Application	Hybertext Transfer	File Transfer	Electronic Mail	Terminal Emulation	Domain Names	File Transfer	Client / Server	Network Management
			Presentation	Hybertext Transfer Protocol (HTTP) RFC 2616	File Transfer Protocol (FTP) RFC 959	Simple Mail Transfer Protocol (SMTP) RFC 2821	TELNET protocol RFC 854	Domain Name System (DNS) RFC 1034-1035	Trivial File Transfer protocol (TFTP) RFC 1350	Sun Microsystems Network File System (NFS) RFC 3530	Simple Network Management Protocol (SNMP) RFC 1157, 1901-10 & 3411-18
	Logical Connectivity		Session								
	Internetwork Connectivity	Host-to-Host	Transport	Transmission Control Protocol (TCP) RFC 793				User Datagram Protocol (UDP) RCF 768			
Communication Subnet		Internet	Network	Address Resolution ARP - RFC 826 RARP - RFC 903		Internet Protocol (IP) RFC 791			Internet Control Message Protocol (ICMP) RFC 792		
	Local Network Connectivity	Network Interface	Data Link	Network Interface Cards: Ethernet, Token Ring, MAN (metropolitan area network) and WAN (wide area network) RFC 894, 1042 etc.							
			Physical	Transmission Media: Twisted Pair, Coax, Fiber Optics, Satellites, Wireless Media etc.							

Table 2.6: ARPA – OSI Layers (Partly from Mark A. Miller, Internet Technologies Handbook 9 and 22-23)

- The **Physical Layer** handles transmission of unstructured bits stream (the physical interface) between one node a data transmission device (e.g., workstation, computer) and the next transmission medium or network. The Physical Layer functions is concerned with specifying the characteristics of interfacing with the transmission media; the nature of the signals and encoding the data signal; defining the range of the voltage or current magnitudes; defining the connector sizes, shapes, and pinouts; and anything generally associated with the physical transmission of the bit stream.
- The **Data Link Layer** maintains a reliable communication link between adjacent nodes. It is concerned with the exchange of data in blocks (frames), access to and routing data across a network for two end systems (server, workstation, etc.) attached to the same network. As such, it assumes that the Physical Layer is noisy or prone to errors. The Data Link Layer inserts addresses in the data frame (including source and destination) and provides error and flow control for the data - usually implemented with a Cyclic Redundancy Check (CRC). The sending computer may wish to invoke certain services, such as priority, that might be provided by the network. The specific software used at this layer depends on the type of network to be used; different standards have been developed for circuit switching, packet switching (e.g., frame relay), LANs (e.g., Ethernet), and others. The same higher-layer software should function properly regardless of the particular network to which the computer is attached.
- On **Transport/Host-to-Host Layer** and **Network/Internet Layer**, see full text.
- The **Session Layer** establishes, manages, and terminates process-to-process communication sessions between hosts (with cooperating applications). Translation between name and ad-dress databases, as well as synchronization between the two hosts, may be required to manage the sessions.
- The **Presentation Layer** establishes the syntax (or form) in which data is exchanged between the two hosts. As such, the Presentation Layer provides a data manipulation function, not a communication function. Data compression and data encryption are two examples of Presentation Layer services.
- The **Application Layer** contains the logic needed to support the various user applications and provides end-user services, such as Application Layer file transfers, electronic messages, virtual terminal emulation, remote database access, and network management. The end user interacts with the Application Layer. For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application. At the application layer, the packet consists simply of the data to be transferred.

2.3.1. Some Network Terms

An interconnected set of networks, from a user's point of view, may appear simply as a larger network. However, if each of the constituent networks retains its identity, and special mechanisms are needed for communicating across multiple networks, then the entire configuration is often referred to as an "internet", and each of the constituent networks as a "subnetwork". The most important example of an internet is referred to simply as the Internet. It has served as the basis for the development of internetworking technology and as the model for private internets within organizations. These latter are also referred to as "intranets".

Each constituent subnetwork in an internet supports communication among the devices attached to that subnetwork. These devices are referred to as End Systems (ESs). In addition, subnetworks are connected by devices referred to in the ISO documents as Intermediate Systems (ISs). ISs provide a communications path and perform the necessary relaying and routing functions so that data can be exchanged between devices attached to different subnetworks in the internet.

Two types of ISs of particular interest are "bridges" and "routers". The differences between them have to do with the types of protocols used for the internetworking logic. Both the bridge and the router assume that the same upper-layer protocols are in use. Thus, the internet is collection of communication networks interconnected by bridges and/or routers

In essence, a bridge operates at the Data Link Layer of the OSI seven-layer architecture and acts as a relay of frames[57] between like networks. It is an IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet.

A router is a processor that connects two networks (through their gate-

[57] A frame is the unit of transmission in a link layer protocol, and consists of a link-layer header followed by a packet, RFC 1122 *supra* note 7, at 17.

ways) and whose primarily function is to relay data from one network to the other on its route from the source to the destination end system. It operates at the Network Layer of the OSI architecture and routes packets between potentially different networks that may or may not be similar. The router employs an Internet protocol present in each router and each end system of the network. There are different kinds of routers.

An ordinary router simply looks at the destination address of each packet and picks the best way it knows to send that packet towards that destination. The decision about how to handle the packet is based solely on its destination.

A screening router looks at packets more closely by determining whether or not it can route a packet towards its destination. It also determines whether or not it should.

Once it has looked at all the information, a straightforward packet-filtering router can do any of the following things:

- send the packet on to the destination is was bound for
- drop the packet (without sending a message to the sender)
- reject the packet (and return an error to the sender)
- log information about the packet
- set off an alarm to notify somebody about the packet immediately

Routers that are more sophisticated can also:[58]

- modify the packet (e.g. to do network address translation)
- send the packet on to a destination other than the one that it was bound for (e.g. to force transactions through a proxy server or perform load balancing)
- modify the filtering rules (e.g. to accept replies to a UDP packet or to deny all traffic from a site that has sent hostile packets).

[58] E.g. a Packet Filtering Bridge, which is a packet filtering device that pay attention only to "should" or "should not" and have no ability route. It's a dedicated security device, which is harder to detect and attack than packed filtering routers; Stateful Packet Filters (= Dynamic packet filters), which is a packet filtering devices that keep track of packets that they see. They keep information about the state of transactions and change their handling of packets dynamically depending on the traffic they see. There are also so-called Intelligent Packet Filters, which look at the content of packets rather than at just their headers.

The router's main task is to route messages on the network. Connectionless protocols, such as IPv4 and IPv6, use a technique know as routing by network address. When a packet reaches a router through a local or a geographical network interface, the router passes the packet to its forwarding process, which extracts the source address, uses this address to examine the routing tables, and decides on which interface to retransmit the packet. The IPv6 contains one entry for each subnetwork reachable from the router itself.[59]

Thus, Internetworking among dissimilar subnetworks is achieved by using routers to interconnect the subnetworks. Essential functions that the router must perform include the following:

- Provide a link between networks.
- Provide for the routing and delivery of data between processes on end systems attached to different networks.
- Provide these functions in such a way as not to require modifications of the networking architecture of any of the attached subnetworks.

The third point implies that the router must accommodate a number of differences among networks, such as the following:

- Addressing schemes: The networks may use different schemes for assigning addresses to devices. Some form of global network addressing must be provided, as well as a directory service.
- Maximum packet sizes: Packets from one network may have to be broken into smaller pieces to be transmitted on another network, a process known as "segmentation".
- Interfaces: The hardware and software interfaces to various networks differ. The concept of a router must be independent of these differences.
- Reliability: Various network services may provide anything from a reliable end-to-end virtual circuit to an unreliable service. The operation of the routers should not depend on an assumption of network reliability.

[59] SILVANO GAI, INTERNETWORKING IPV6 WITH CISCO ROUTERS 26-27, available online at <www.ip6.com/us/book/Chap2.pdf> (last modified June 2004) (visited September 2005) [hereinafter SILVANO].

The preceding requirements are best satisfied by an internetworking protocol, such as IP, that is implemented in all end systems and routers. It acts as a relay to move a block of data from one host, through one or more routers, to another host.[60] TCP is implemented only in the end systems; it keeps track of the blocks of data to assure that all are delivered reliably to the appropriate application.

For successful communication, every entity in the overall system must have a unique address. Actually, two levels of addressing are needed. Each host on a sub-network must have a unique global internet address;[61] this allows the data to be delivered to the proper host. Each process with a host must have an address that is unique within the host; this allows the host-to-host protocol (TCP) to deliver data to the proper process. These latter addresses are known as "ports".

"Tunneling" - or "encapsulation" - is a process whereby information from one protocol is encapsulated inside the frame or packet of another architecture,[62] thus enabling original data to be carried over that second architecture, for example between IPv4 and IPv6.[63] The tunneling process involves three distinct steps:[64]

[60] RFC 791 *supra* note 32 and P. Almquist, *Type of Service in the Internet Protocol Suite*, RFC 1349 (July 1992).

[61] On New Domain Name System Extensions, see RCF 1886.

[62] For example the Layer Two Tunneling Protocol [L2TP] provides a method for tunneling PPP [Point-to-Point] packets. Working in the Data Link Layer of the OSI model, PPP sends the computer's TCP/IP packets to a server that puts them onto the Internet. PPP is a method of connecting a computer to the Internet that provides error checking features. See, J. Lau, M. Townsley & I. Goyret (Editors), *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*, RFC 3931 (March 2005) and W. Townsley, *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update*, RFC 3438 (December 2002).

[63] B. Carpenter & C. Jung, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*, RFC 2529 (March 1999) & B. Carpenter & K. Moore & B. Fink, *Routing IPv6 over IPv4 – Connecting IPv6 Routing Domains Over the IPv4 Internet*, at <http://www.cisco.com/en/US/about/ac123/ac147/ac174/ac197/about_cisco_ipj_archive_article09186a00800c830a.html> (visited October 2005).

[64] A. Conta & S. Deering, *Generic Packet Tunneling in IPv6 – Specification*, RFC 2473 (December 1998).

- Encapsulation – at the encapsulation node (or tunnel entry point) the IPv4 header is created and the encapsulated packet is transmitted. This node may maintain configuration information regarding the tunnels that are established, such as the maximum transfer unit (MTU) size that is supported in that tunnel.
- Decapsulation – at the decapsulation node (or tunnel exit point) the IPv4 header is removed and the IPv6 packet is processed.
- Tunnel Management

RFC 2893 defines four possible tunnel configurations that could be established between routers and hosts.[65]

IP-level security encompasses two functional areas: authentication and privacy:[66]

- The authentication mechanism ensures that a received packet was in fact transmitted by the party identified as the source in the packet header. In addition, this mechanism ensures that the packet has not been altered in transit.
- The privacy facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.

A key concept that appears in both the authentication and privacy mechanisms for IP is the security "association". An association is a one-way relationship between a sender and a receiver. It is necessary to encapsulate the entire block (ESP header plus encrypted IP packet) with a new IP header that will contain sufficient information for routing but not for traffic analysis.

2.3.2. Basic Requirements in the Internet Architecture Suit

The Internet Layer is based on the Robustness Principle: "Be liberal in what you accept, and conservative in what you send."[67]

[65] R. Gilligan & E. Nordmark, *Transition Mechanisms for IPv6 Hosts and Routers*, RFC 2893 (August 2000) & K. Kompella, *A Traffic Engineering (TE) MIB* [Management Information Base], RFC 3970 (January 2005) & MILLER *supra* note 6, at 250-260.

[66] William Stallings, *IPv6: The New Internet Protocol*, at <http://www.cs-ipv6.ac.uk/ipv6/documents/papers/Stallings> (visited January 2005) [hereinafter STALLINGS-2].

[67] RFC 1122 *supra* note 7, at 26.

The basic assumptions any host must follow are:[68]

- The Internet is a network of networks.
- Gateways don't keep connection state information - To improve robustness of the communication system, gateways are designed to be stateless, forwarding each IP datagram independently of other datagrams. As a result, redundant paths can be exploited to provide robust service in spite of failures of intervening gateways and networks.

  All state information required for end-to-end flow control and reliability is implemented in the hosts, in the transport layer or in application programs. All connection control information is thus colocated with the end points of the communication, so it will be lost only if an end point fails.
- Routing complexity should be in the gateways. - Routing is a complex and difficult problem, and ought to be performed by the gateways, not the hosts. An important objective is to insulate host software from changes caused by the inevitable evolution of the Internet routing architecture.
- The System must tolerate wide network variation - A basic objective of the Internet design is to tolerate a wide range of network characteristics - e.g., bandwidth, delay, packet loss, packet reordering, and maximum packet size. Another objective is robustness against failure of individual networks, gateways, and hosts, using whatever bandwidth is still available. Finally, the goal is full "open system interconnection": an Internet host must be able to interoperate robustly and effectively with any other Internet host, across diverse Internet paths.

  Sometimes host implementors have designed for less ambitious goals. For example, some vendors have fielded host implementations that are adequate for a simple LAN environment, but work badly for general interoperation. However, isolated LANs seldom stay isolated for long; they are soon gatewayed to organization-wide internets, and eventually to the global Internet system. Thus, in the end, neither

[68] RFC 1122 *supra* note 7, at 6-7.

the customer nor the vendor is served by incomplete or substandard Internet host software.

In the Internet Protocol Suite to communicate using the Internet system, a host must implement the layered set of protocols comprising the Internet protocol suite. A host typically must implement at least one protocol from each layer, see Table 2.6.

Any host that forwards datagrams generated by another host is acting as a gateway and must also meet the specifications laid out in "Requirements for Internet Gateways"[69].

For normal incoming datagrams the IP layer:[70]

- Verifies that the datagram is correctly formatted
- Verifiers that it is destined to the local host
- Processes options
- Reassembles the datagram If necessary, and
- Passes the encapsulated massage to the appropriate transport-layer protocol module.

For outgoing datagrams the IP layer:

- Sets any fileds no set by the transport layer
- Selects the correct first hop on the connected network ("routing")
- Fragments the datagram if necessary and if intentional fragmentation is implemented, and
- Passes the packet(s) to the appropriate link-layer driver.

2.4. IPv4 of 1983

The main protocol between network entities that make the Internet works is the Internet Protocol from 1983 (IP version 4). It can be described with reference to the IP datagram format, which contains the following fields (see table 2.4):

- **Version** (4 bits): Indicates version number, to allow evolution of the protocol; the value is 4.

[69] J. Reynolds & J. Postel, *The Request for Comments Reference Guide*, RFC 1000 (August 1987).

[70] FRC 1122 *supra* note 7, at 27.

- **Internet Header Length** (IHL) (4 bits): Length of header in 32-bit words. The minimum value is five, for a minimum header length of 20 octets.
- **Type of Service** (8 bits): Provides guidance to end-system IP modules and to routers along the datagram's path. It consists of two subfields:
  a. TOS Subfield - The subfield is set by the source system to indicate the type or quality of service that should be provided. In practice, routers may ignore this field. The lists requirement for IPv4 routers is given in RFC 1812.[71] However, a router may abandon a datagram even though a route is available, because there is no route with either the same TOS or normal service. The encoding for this subfield as defined in RFC 1349[72] is:
     - 1000 - Minimize delay
     - 0100 - Maximize throughput
     - 0010 - Maximize reliability
     - 0001 - Minimize monetary cost
     - 0000 – Normal Service

  b. Precedence Subfield - The subfield indicated the degree of urgency or priority to the be associated with a datagram. However, routers may disregard this subfield. The encoding for this subfield as defined in RFC 1349 is:
     - 111 - Network control
     - 110 - Internetwork control
     - 101 - Critical
     - 100 - Flash override
     - 011 - Flash
     - 010 - Immediate
     - 001 - Priority
     - 000 - Routine

     The recommendations in RFC 1812, which fall into two categories:

[71] F. Baker (Ed.), *Requirements for IP Version 4 Routers*, RFC 1812 (1995).
[72] RFC 1349 *supra* note 60.

i. Queue Service:[73]

Routers should implement precedence-ordered queue service.

Any router may implement other policy-based throughput management procedures that result in other than strict precedence ordering, but it must be configurable to suppress them.

ii. Congestion Control:[74]

When a router receives a packet beyond its storage capacity, it must discard it or some other packet or packets

A router may discard the packet it has just received; this is the simplest but not the best policy.

Ideally, the router should select a packet from one of the sessions most heavily abusing the link, given that the applicable quality-of-service policy permits this.

If precedence-ordered queue service is implemented and enabled, the router must not discard a packet whose IP precedence is higher than that of a packet that is not discarded.

A router may protect packets whose IP headers request the maximize reliability TOS, except where doing so would be in violation of the previous rule.

A router may protect fragmented IP packets, on the theory that dropping a fragment of a datagram may increase congestion by causing all fragments of the datagram to be retransmitted by the source.

To help prevent routing perturbations or disruption of management functions, the router may protect packets used for routing control, link control, or network management from being discarded.

[73] *Id.* 87 et. al.
[74] *Id.* 94 et. al.

- **Total Length** (16 bits): Total length of this fragment, in octets.
- Identification (16 bits): A sequence number that, together with the source address, destination address, and user protocol, is intended to identify a datagram uniquely. Thus, the identifier should be unique for the datagram's source address, destination address, and user protocol for the time during which the datagram will remain in the internet.
- **Flags** (3 bits): Only two of the bits are currently defined. When a datagram is fragmented, a "More bit" indicates whether this is the last fragment in the original datagram. A "Don't Fragment bit" prohibits fragmentation when set. This bit may be useful if it is known that the destination does not have the capability to reassemble fragments. However, if this bit is set, the datagram will be discarded if it exceeds the maximum size of an en route subnetwork. Therefore, if the bit is set, it may be advisable to use source routing to avoid subnetworks with small maximum packet size.
- **Fragment Offset** (13 bits): Indicates where in the original datagram this fragment belongs, measured in 64-bit units. This implies that fragments other than the last fragment must contain a data field that is a multiple of 64 bits in length. See further below.
- **Time to Live** (8 bits): Specifies how long, in seconds, a datagram is allowed to remain in the internet. Every router that processes a datagram must decrease the TTL by at least one, so the TTL is somewhat similar to a hop count. See further below.
- **Protocol** (8 bits): Indicates the next higher level protocol, which is to receive the data field at the destination; thus, this field identifies the type of the next header in the packet after the IP header.
- **Header Checksum** (16 bits): An error-detecting code applied to the header only. Because some header fields may change during transit (e.g., time to live, segmentation-related fields), this is reverified and recomputed at each router. The checksum field is the 16-bit ones complement addition of all 16-bit words in the header. For purposes of computation, the checksum field is itself initialized to a value of zero.
- **Source Address** (32 bits): Coded to allow a variable allocation of bits to specify the network and the end system attached to the specified network (7 and 24 bits, 14 and 16 bits, or 21 and 8 bits). See further below.
- **Destination Address** (32 bits): Same characteristics as source address. See further below.

- **Options** (variable): Encodes the options requested by the sending user. In this field can be made a sequenced list of router addresses that specifies the route to be followed.
- **Padding** (variable): Used to ensure that the datagram header is a multiple of 32 bits in length.
- **Data** (variable): The data field must be an integer multiple of 8 bits in length. The maximum length of the datagram (data field plus header) is 65,535 octets.

In IP, datagram fragments are reassembled at the destination end system. The IP fragmentation technique uses the following information from the IP header, see table 2.5 above:

- Identification (ID)
- Data Length (difference between total length and Internet header length)
- Fragment Offset
- More Flag

To fragment a long datagram, an IP module in a router performs the following tasks:

- Create two new datagrams and copy the header fields of the incoming datagram into both.
- Divide the incoming user data field into two approximately equal portions along a 64-bit boundary, placing one portion in each new datagram. The first portion must be a multiple of 64 bits.
- Set the Data Length of the first new datagram to the length of the inserted data, and set More Flag to 1 (true). The Offset field is unchanged.
- Set the Data Length of the second new datagram to the length of the inserted data, and add the length of the first data portion divided by 8 to the Offset field. The More Flag remains the same.

As fragments with the same ID arrive, their data fields are inserted in the proper position in the buffer until the entire data field is reassembled, which is achieved when a contiguous set of data exists starting with an Offset of zero and ending with data from a fragment with a false More Flag.

The IPv4 service does not guarantee delivery. Some means is needed to decide to abandon a reassembly effort to free up buffer space. Two approaches are commonly used. First, assign a reassembly lifetime to the first fragment to arrive. This is a local, real-time clock assigned by the reassembly function and decremented while the fragments of the original datagram are being buffered. If the time expires prior to complete reassembly, the received fragments are discarded. A second approach is to make use of the datagram

lifetime, which is part of the header of each incoming fragment. The Lifetime field continues to be decremented by the reassembly function; as with the first approach, if the lifetime expires prior to complete reassembly, the received fragments are discarded.

The source and destination address fields in the IPv4 header each contain a 32-bit global internet address, generally consisting of a network identifier and a host identifier. The format of the addresses is such that it is possible to mix the following three classes of addresses on the same internetwork.[75]

- Class A: Few networks, each with many hosts – Network addresses begin a first octet with 0-127
- Class B: Medium number of networks, each with a medium number of hosts – Network addresses begin a first octet with 128-191
- Class C: Many networks, each with a few hosts – Network addresses begin a first octet with 192-223

In IPv4, addresses generally do not have a structure that assists routing, and therefore a router may need to maintain a huge table of routing paths.

2.5. IPv6 of 1996

Even though the present version IPv4 has been the standard for decades, there has already been made a new version of the IP-protocol,[76] since the IPv4 has many serious limits that a new version from 1996 (IPv6[77]) has been designed

[75] RFC 1812 *supra* note 71, at, 20 et. al.

[76] Current specification: S. Deering, & H. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460 (December 1998), confer *IPng Current Specifications* (last updated September 21, 2001) at <http://playground.sun.com/pub/ipng/html/specs/specifications.html#SPEC> (visited October 2005). See also *ITU and its Activities: Related to Internet-Protocol (IP) Networks*, Version 1.1, April 2004 at <http://www.itu.int/osg/spu/ip/itu-and-activities-related-to-ip-networks-version-1.pdf> (visited March 2006) and *IP Version 6 (IPv6)* (last updated January 3, 2003) at <http://playground.sun.com/pub/ipng/html/#INTRO> (visited October 2005).

[77] STALLINGS-2 *supra* note 66.

to overcome.[78]

The IPv6 header has a fixed length of 40 octets, which contains the following fields (see table 2.5):[79]

- **Version** (4 bits): Internet Protocol version number; the value is 6.
- **Traffic Class** (8 bits): Available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. The use of this field is under consideration.80
- **Flow Label** (20 bits): A flow is a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. A flow is uniquely identified by the combination of a source address, destination address, and a nonzero 20-bit flow label. Hosts or routers that do not support this field must pass the field unchanged when forwarding a packet, and ignore the filed when receiving a packet.
- **Payload Length** (16 bits): Length of the remainder of the IPv6 packet following the header, in octets.
- **Next Header** (8 bits): Identifies the type of header immediately following the IPv6 header, that is, either an IPv6 extension header or a higher-layer header, such as TCP.
- **Hop Limit** (8 bits):81 The remaining number of allowable hops for this packet. The hop limit is set to some desired maximum value by the source and decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero. In general, IPv4 routers treat the time-to-live field as a hop limit field.
- **Source Address** (128 bits): The address of the originator of the

[78] S. Bradner & A. Mankin, *The Recommendation for the IP Next Generation Protocol*, RFC 1752 (January 1995).
[79] RFC 2460 *supra* note 76, at 2-3 and SILVANO *supra* note 59, at Chapter 3.
[80] See RFC 2460 *supra* note 76, at 26.
[81] N. Shen & H. Smit, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*, RFC 3906 (October 2004).

packet. Addresses are assigned to individual interfaces on nodes[82], not to the nodes themselves. Thus, a single interface[83] may have multiple unique unicast addresses. This allows a subscriber that uses multiple access providers across the same interface to have separate addresses aggregated under each provider's address space.

- **Destination Address** (128 bits): The address of the intended recipient of the packet. This may not in fact be the intended ultimate destination if a Routing Header extension is used, see next.

In IPv6, optional Internet Layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There has only been defined the following small number of such extension headers (The above mentioned IPv6 Header has always to be the first header in an IPv6 packet):[84]

- **Hop-by-Hop Options header**: Defines special options that require hop-by-hop processing. The hop-by-hop options header carries optional information that, if present, must be examined by every router along the path.
- **Routing header**: Provides extended routing, similar to IPv4 source routing. The routing header contains a list of one or more intermediate nodes to be visited on the way to a packet's destination.
- **Fragment header**: Contains fragmentation and reassembly information. In IPv6, fragmentation may only be performed by source nodes, not by routers along a packet's delivery path.[85]
- Authentication header: Provides packet integrity and authentication.[86]
- **Encapsulating Security Payload header**: Provides privacy. The use of the ESP provides support for privacy and data integrity for IP

[82] In IPv6 a "node" is any device that implements IPv6, including hosts and routers.

[83] A node's attachment to a link, that is, a communication facility or medium over which nodes can communicate at the Data Link Layer.

[84] RFC 2460 *supra* note 76, at 6-7.

[85] STALLINGS-2 *supra* note 66.

[86] R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 1825 (August 1995), R. Atkinson, *IP Authentication Header*, RFC 1826 (August 1995) & P. Metzger & W. Simpson, *IP Authentication using Keyed MD5*, RFC 1828 (August 1995).

packets. This mechanism can be used to encrypt either a transport-layer segment (e.g., TCP, user data gram protocol - UDP, or ICMP), known as "transport-mode ESP", or an entire IP packet, known as "tunnel-mode ESP".87 The tunnel mode is useful in a configuration that includes a firewall or other sort of security gateway, which protects a trusted network from external networks.88

- **Destination Options header**: Contains optional information to be examined by the destination node.

An example of an IPv6 extension header is the Fragment header that can look as follows:

Next hdr	Reserved	Frag. Offset	Flags
Fragment identifier			

Table 2.7 IPv6 Fragment Header[89]

In IPv6, a node is any device that implements IPv6, that is, IPv6 is implemented in each end system and in routers.[90]

IPv6 allow a subscriber to use multiple access providers across the same interface[91] to have separate addresses aggregated under each provider's address space.

IPv6 allows three types of addresses:[92]

- Unicast: An identifier for a single interface. A unicast address en-

[87] R. Atkinson, *IP Encapsulating Security Payload (ESP)*, RFC 1827, (August 1995) & P. Karn & P. Metzger, *The ESP DES-CBC Transform*, RFC 1829 (August 1995) and RFC 3970 *supra* note 65 and STALLINGS-2 *supra* note 66.

[88] STALLINGS-2 *supra* note 66.

[89] Marc E. Fiuczynsky et. al., *The Design and Implementation of an IPv6/IPv4 Network Address and Protocol Translator*, Section 2.2.1, USENIX Association 1998, <http://www.usenix.org/publications/library/proceedings/usenix98/full_papers/fiuczynski/fiuczynski.pdf#search='Design%20and%20Implementation%20of%20an%20IPv6%2FIPv4%20Network%20Address%20and%20Protocol%20Translator'> (visited October 2005) [hereinafter FIUCZYNSKY]. See also SILVANO *supra* note 59, at 51-53.

[90] STALLINGS-2 *supra* note 66.

[91] The hardware and software interfaces to various networks differ. The concept of a router must be independent of these differences.

[92] STALLINGS-2 *supra* note 66.

ables a single source to specify a single receiver in a network. Thus, a packet sent to a unicast address is delivered to the interface identified by that address. Unicast addresses may be structured in a number of ways. The following have been identified:

- provider-based global
- link-local, site-local
- IPv4-compatible IPv6
- loopback[93]

- Anycast: An identifier for a set of interfaces (typically belonging to different nodes). An anycast address enables a single source to specify that it wants to contact any one node from a group of nodes via a single address. A packet with such an address will be routed to the nearest interface in the group, according to the routing protocols' measure of distance. It is designed to let one host initiate the efficient updating of router tables for a group of hosts.
- Multicast: An identifier for a set of interfaces (typically belonging to different nodes). A multicast address enables a single source to specified multiple receivers. Thus, IPv6 includes the capability to address a predefined group of interfaces with a single multicast address. A packet with a multicast address is to be delivered to all interfaces identified by that address (all members of the group).

2.6. Some differences between the two IP-versions

Years ago, the world ran out of IPv4 addresses for networked devices because IPv4 only supports about 2.000.000.000 addresses and with an enormous waste of usable addresses. Furthermore, the Internet is increasingly becoming a multimedia, application-rich, and complex client/server environment. All of these developments have outstripped the capability of IPv4-based networks to supply needed functions and services. An internetworked

[93] Loopback is a test mechanism of network adapters. 127.0.0.1 is the loopback address in IP. IP applications often use this feature to test the behavior of their network interface. Messages sent to 127.0.0.1 do not get delivered to the network. Instead, the adapter intercepts all loopback messages and returns them to the sending application.

environment needs to support real-time traffic, flexible congestion control schemes, and security features. None of these requirements is easily met with the existing IPv4.[94]

Ultimately, all installations using TCP/IP are expected to implement IPv6 or may be even to change from the current IPv4 to IPv6,[95] but this process will take many decades.[96]

The following is a broad overview of differences and similarities which can affect the possibilities for States to legislate what is transmitted on international computer networks.

The strength of the IPv4 have been providing a service with the following main characteristics that also have become its main limits and forcing the introduction of IPv6:[97]

- Universal addressing – enact IPv4 network interface has a unique worldwide address with 32 bits
- Best effort – IPv4 performs its best effort to deliver packets, but it doesn't guarantee anything at the upper layer, neither in terms of percentage of delivered packets nor in terms of time used to execute the delivery. In short, IPv4 doesn't have a built-in concept of Quality of Service (QoS).

The IPv6 is a protocol with an extremely pure design and a small header with few fields.

IPv6 provides a larger address space than IPv4 (128 bits in length to 32

[94] STALLINGS-2 *supra* note 66.

[95] STALLINGS-1, *supra* note 41, at 31.

[96] The U.S. Department of Defense has stated that it plans a full migration to IPv6 by 2008. Additionally, a substantial investment in the development of new training materials for government employees will be required to meet the 2008 deadline, Press Release, *Defense Department Will Require IPv6 Compliance, Says DoD's John Osterholz*, MARKET WIRE, June 26 2003, at <http://www.findarticles.com/p/articles/mi_pwwi/is_200306/ai_mark1060030660> (visited October 2005) and Sean Convery & Darrin Miler, *IPv6 and IPv4 Threats Comparison and Best-Practice Evaluation (v1.)* page 2, at <http://www.cisco.com/security_services/ ciag/documents/v6-v4-threats.pdf#search='ipv4%20sean%20convery'> (visited October 21, 2005) [hereinafter CONVERY].

[97] SILVANO *supra* note 59, at 2 and 15-16.

bits) and uses a wiser address allocation policy – so-called Classless Inter-Domain Routing (CIDR)[98] - which minimize the growth of routing tables, and provides more than a billion of billions addresses per square meter on the Earth.[99]

The numbers of fields in the IPv6 packet header are reduced from IPv4 (8 versus 12). The IPv6 packet header has a fixed-length size with a length of 40 octets, whereas the IPv4 header is variable-length. Thus, routers have less processing to do per header in IPv6, which should speed up routing – unless extension headers are used.

The IPv6 design simplifies processing. In IPv6, fragmentation may only be performed by the source.[100] In addition, the IPv6 has been designed to satisfy the growing need of security by allowing the receiver to be reasonably sure about the origin of the data with use of end-to-end encryption of data at the Internet Layer. Thus, IP spoofing[101] attacks and eavesdropping of data will be much more difficult. However, network-level encryption poses new security problems. Another problem is that decryption puts a considerable overload on the CPU and leaves the host more vulnerable to flooding-type DoS attacks.[102]

[98] Y. Rekhter, *CIDR and Classful Routing*, RFC 1817 (August 1995).

[99] D. Plonka, *Embedding Globally-Routable Internet Addresses Considered Harmful*, RFC 4085 (June 2005), M. Duerst, *Internationalized Resource Identifiers (IRIs)*, RFC 3987 (January 2005), T. Berners-Lee & R. Fielding, *Uniform Resource Identifier (URI): Generic Syntax*, RFC 3986 (January 2005), G. Camarillo, *The Internet Assigned Number Authority (IANA) - Header Field Parameter Registry for the Session Initiation Protocol (SIP)*, RFC 3968 (December 2004).

[100] STALLINGS-2 *supra* note 66.

[101] IP Spoofing - A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. Newer routers and firewall arrangements can offer protection against IP spoofing.

[102] D. Turk, *Configuring BGP to Block Denial-of-Service Attacks*, RFC 3882 (September 2004) & P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, RFC 2827 (May 2000) & P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, RFC 2267 (January 1998).

2.6.1. IP Security - Attacks

The same problems that plague IPv4 Security (IPsec) deployment will affect IPv6 IPsec deployment. Therefore, IPv6 is usually deployed without cryptographic protections of any kind. It should be noted that most security breaches occur at the application level (see Table 2.6).[103]

However, some significant differences exist between IPv4 and IPv6. The following nine attacks have substantial differences when moved to an IPv6 world. In some cases the attacks are easier, in some cases more difficult, and in others only the method changes. Thus, these methods can also be used by States in their Information Warfare strategies.[104] At the same time, the possibility of the following attacks show the vulnerability of the network and thus ways to circumvent a State's attempt to legislate ("borders" on) computer networks by code.

- **Reconnaissance** - Generally the first attack executed by an adversary. In this attack the adversary attempts to learn as much as possible about the victim network. This includes both active network methods such as scanning as well as more passive data mining such as through search engines or public documents. In IPv4 the adversary has several well-established methods of collecting this information:
    - Ping sweeps — By determining the IPv4 addresses in use at an organization (through active probes, whois lookups, and educated guesses), an adversary can systematically sweep a network with ICMP or Transport Layer "ping" messages that solicit a reply, assuming both query and response are not filtered at the network border. Following this scan, the adversary uses the data to formulate some hypothesis regarding the layout of the victim network.

[103] CONVERY *supra* note 96, at 2-21, and P. Savola & C. Patel, *Security Considerations for 6to4*, RFC 3964 (December 2004). See also Security Threat Management Report 2005 (Sophus) at <www.securitymanagement.com/library/trojans_sophos0206.pdf> (visited May 2006) and Stephen J. Lukasik, *Current and Future Technical Capabilities in* SOFAER *supra* note 3, at 125. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/125.pdf>.

[104] SPANG-HANSSEN *supra* note 12, Chapter 14.

Tools such as traceroute and firewalk can provide further data to aid the adversary.

- Port scans — After identifying reachable systems, the adversary can systematically probe these systems on any number of Transport Layer ports to find services both active and reachable. By discovering hosts with active services, the adversary can then move to the next phase.
- Application and vulnerability scans — The adversary can then probe these active ports by various means to determine the operating system and the version numbers of applications running on the hosts, and even test for the presence of certain well-known vulnerabilities.

IPv6 reconnaissance is different from IPv4 reconnaissance in two major ways. The first is that the ping sweep or port scan, when used to enumerate the hosts on a subnet, are much more difficult to complete in an IPv6 network. The second is that new multicast addresses in IPv6 enable an adversary to find a certain set of key systems (for example routers, Network Time Protocol (NTP) servers) more easily. Beyond these two differences, reconnaissance techniques in IPv6 are the same as in IPv4. Additionally, IPv6 networks are even more dependent on ICMPv6 to function properly.[105] Aggressive filtering of ICMPv6 can have negative effects on network functions.

The default subnet size of an IPv6 subnet is 64 bits, or 264, versus the most common subnet size in IPv4 of 8 bits, or 2. This increases the scan size to check each host on a subnet by 264 - 28 (approximately 18 quintillion). Thus, a network that ordinarily required only the sending of 256 probes now requires sending more than 18 quintillion probes to cover an entire subnet. It would take more than 28 years of constant scanning to find the first active host, assuming the first success occurs after iterating through 50 percent of the first 1.8 quadrillion addresses. However, many variables can make this scanning easier for the adversary:

[105] A. Conta & S. Deering, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) – Specification*, RFC 2463 (December 1998).

- First, public services on the Internet edge need to be reachable with DNS.
- Second, the large nature of IPv6 addresses and the lack of a strict requirement for Network Address Translation (NAT)[106] will cause more networks to adopt dynamic DNS or other mechanisms to ensure that even hosts have a valid DNS name
- Third, administrators may opt for easy-to-remember host addresses for key systems
- Fourth, by exploiting poorly secured routers or other gateway devices, an adversary could view the IPv6 neighbor-discovery cache data (the functional equivalent of an ARP[107] cache) to find available hosts, or could simply turn on a packet-capture capability such as tcpdump to find addresses available to scan.

Like in IPv4 networks, the internal hosts should be protected by a firewall that limits or completely prevents uninitiated conversations from reaching these systems.

IPv6 supports new multicast addresses that can enable an adversary to identify key resources on a network and then attack them. It becomes critical that these internal-use addresses are filtered at the border and not reachable from the outside.

Today there is no known ping sweep tool for IPv6.[108]

Reconnaissance techniques are generally limited to filtering certain types of messages. Reconnaissance activity cannot be stopped completely because the very act of permitting communications with ones owns devices permits some form of reconnaissance.

[106] B. Aboba & W. Dixon, *IPsec-Network Address Translation (NAT) Compatibility Requirements*, RFC 3715 (March 2004).

[107] Address Resolution Protocol – a protocol for mapping an Internet protocol address (IP address) to a physical machine address that is recognized in the local network. At a gateway the ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.

[108] CONVERY *supra* note 96.

- **Unauthorized access** - Refers to the class of attacks where the adversary is trying to exploit the open transport policy inherent in the IP protocol. Nothing in the IP protocol stack limits the set of hosts that can establish connectivity to another host on an IP network. Attackers rely upon this fact to establish connectivity to upper-layer protocols and applications on internetworking devices and end hosts.

  The need for access control technologies is the same in IPv6 as in IPv4. The addressing system of IPv6 changes from that for IPv4 because it includes the ability for one adapter in an IPv6-enabled node to have multiple IPv6 addresses. In IPv6 the network designer can assign global unicast addresses only to devices that need to communicate with the global Internet while assigning site-local addresses to devices that need to communicate only within the organization.

  Numerous significant technology and threat differences between the IPv6 and IPv4 headers may change how an administrator deploys these technologies.

  IP options in IPv4 are replaced with extension headers in IPv6. With this replacement, extension headers may be used in an attempt to circumvent security policy.

  Currently most IPv4 firewalls do minimal multicast inspection and filtering. Local-use multicast is integral to the functioning of IPv6.

  Firewalls in Internet Layer mode should never forward link-layer multicasts. Devices acting as firewalls should inspect all source IPv6 addresses and filter any packets with a multicast source address.

  Any stateful device needs to make feature enhancements to its code to be able to be able to designate an anycast address for inspection and origin servers that listen and respond to the anycast address.

  In IPv6 transparent firewalls need to enhance their inspection capabilities to inspect the appropriate IPv6 ICMP and multicast messages.

  Some IPv6 firewalls understand only a subset of the extension headers in IPv6, and they drop IPv6 traffic that includes these headers.

- **Header manipulation and fragmentation attacks**. First purpose is to evade network security devices. The second purpose is to use fragmentation or other header manipulation to attack the networking infrastructure directly.

  IPv4 fragmentation[109] has been used as a technique to bypass access controls on devices such as routers and firewalls.

  The combination of multiple extension headers and fragmentation in IPv6 creates the potential that the Transport Layer protocol is not included in the first packet of a fragment set, making it difficult to enforce Transport Layer policy on devices that do not do fragment reassembly.
- **Internet Layer and Transport Layer spoofing**[110] - The ability for an adversary to modify their source IP address and the ports they are communicating on to appear as though traffic initiated from another location or another application.

  Today in IPv4, spoofing attacks (principally Internet Layer-based) occur every day. They can make DoS, spam, and worm or virus attacks more difficult to track down.

  One of the most promising benefits of IPv6 from an Internet Layer spoofing perspective is the globally aggregated nature of IPv6 addresses. Unlike IPv4, the IPv6 allocations are set up in such a way as to easily be summarized at different points in the network.

  The various tunneling mechanisms offer the ability for an adversary with either IPv4 or IPv6 connectivity to send traffic to the other version of IP while masking the true source. As an example, adversaries can use 6to4 relay routers to inject traffic into an IPv6 network with very little ability to trace back to the true source.

  Currently Internet Layer spoofing can be mitigated using the same techniques as in IPv4 with standard ACLs.[111] Transport Layer

[109] IPv4 fragmentation is a technique used to fit the IPv4 datagram into the smallest maximum transfer unit on the path between end hosts.

[110] See *supra* note 102.

[111] Access Control List - a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies

spoofing is not changed in any way. Spoofed traffic can be detected using IPv6-capable firewalls or IDSs.[112]

- **Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks** - ARP and DHCP[113] attacks attempt to subvert the host initialization process or a device that a host accesses for transit. These attacks try to get end hosts to communicate with an unauthorized or compromised device or to be configured with incorrect network information such as default gateway, DNS server IP addresses.

  In IPv6 no inherent security is added on to the IPv6 equivalents of DHCP or ARP. In IPv6 ARP is replaced with elements of ICMPv6 called neighbor discovery. Neighbor discovery has the same inherent security as ARP in IPv4.

  Currently no security tools are available today to help detect or stop DHCPv6, autoconfiguration, or neighbor-discovery abuses in IPv6.
- **Broadcast amplification attacks (smurf)** - a DoS attack tool that takes advantage of the ability to send an echo-request message with a destination address of a subnet broadcast and a spoofed source address, using the victim's IP. All end hosts on the subnet respond to the spoofed source address and flood the victim with echo-reply messages
- **Routing attacks** - Routing attacks focus on disrupting or redirecting traffic flow in a network. This is accomplished in a variety of ways, ranging from flooding attacks, rapid announcement and removal of routes, and bogus announcement of routes.

  No security tools are available today to help detect or stop DHCPv6, autoconfiguration, or neighbor-discovery abuses in IPv6.

which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute.

[112] An Intrusion Detection System inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

[113] A communications protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol addresses in an organization's network.

Routing attacks focus on disrupting or redirecting traffic flow in a network. This is accomplished in a variety of ways, ranging from flooding attacks, rapid announcement and removal of routes, and bogus announcement of routes. Particulars of the attacks vary, depending on the protocol being used.

In IPv4, routing protocols are commonly protected using cryptographic authentication to secure the routing announcements between peers.

Several protocols do not change their security mechanism when transitioning from IPv4 to IPv6.[114]

- **Viruses and worms** - In IPv4, viruses and worms not only damage the hosts themselves but also can damage the transport of the network through the increased burden to routers and mail servers around the Internet.

  A traditional virus in no way changes with IPv6. E-mail based viruses or those that infect removable media remain as you would expect. However, worms or viruses and worms that use some form of Internet scanning to find vulnerable hosts may experience significant barriers to propagation in IPv6.

  The mitigation techniques currently used in IPv4 are al still available in IPv6.
- **Transition, translation, and tunneling mechanisms** – see next subsection.

The following types of attacks has strong IPv4 and IPv6 similarities,[115] thus has not been fundamentally altered by IPv6:

- Sniffing - Sniffing involves capturing data in transit across a network.
- Application layer attacks
- Rogue devices - Rogue devices are devices introduced into the network that are not authorized.
- Man-in-the-middle attacks - The IPv4 and IPv6 headers have no security mechanisms themselves. IPv6 falls prey to the same security

[114] RFC 2893 *supra* note 65 and CONVERY *supra* note 96, at 18.
[115] CONVERY *supra* note 96, at 20-21.

risks posed by a man in the middle attacking the IPsec protocol suite.

- Flooding - The increase in IP addresses that can be spoofed may make flooding attacks more difficult to trace, the core principles of a flooding attack remain the same in IPv6.

2.6.2. 4to6 & 6to4

As it will take decades before every device in the world connected to the Internet will have shifted from IPv4 to IPv6, translation at the Internet Layer is required for a very long time. Thus, when something is originally sent by use of IPv6 but is sent through IPv4-routers, transformation between the two protocols has to be done – and visa versa. Table 2.8 indicates a way this can be done:[116]

[116] E. Nordmark & R. Gilligan, *Basic Transition Mechanisms for IPv6 Hosts and Routers*, RFC 4213 (October 2005).

IPv6	V6 → v4	V6 ← v4	IPv4
Version	Translation	Translation	Version
Priority / class	Not translated	Not translated	
Flow label	Not translated	Not translated	
Payload length	Translation	Translation	
Next Header (extension or protocol)	Directly copied	Directly copied	Protocol
Hop Limit	Directly copied	Directly copied	Time to Live
Next hdr (frag)	Translation	Translation	
Reserved	Not translated	Not translated	
Frag. identifier	Translation	Translation	
	Translation	Translation	Internet Header Length
	Not translated	Not translated	Type of Service
	Translation	Translation	Total Length
	Translation	Translation	Frag. Identification
	Translation	Translation	Flags
	Translation	Translation	Fragment Offset
	Computerized in translation	Ignored	Header Checksum
Source Address	Translation	Translation	Source Address
Destination Address	Translation	Translation	Destination Address
			Options + Padding
(Data)			(*Data)*

Table 2.8 Comparison of IPv4 & IPv6 Headers[117]

Support for features such as authentication (the *authentication header*) and for privacy (the *encapsulating security payload* (ESP) header) is mandatory for IPv6 and optional for IPv4. In both cases, the security features are implemented as extension headers that follow the main IP header.[118]

[117] FIUCZYNSKY *supra* note 89, at Section 2.2.1.
[118] STALLINGS-2 *supra* note 66.

As for transition[119], translation, and tunneling[120] mechanisms, several approaches to transitioning from IPv4 to IPv6 networks exist. These approaches fall into the following categories:[121]

- Dual stack[122]
- Tunneling (see above section 2.3.1)
- Translation (see above Table 2.8)

The following issues can be listed:

- With regard to IPv6 tunneling technologies and firewalls, if the network designer does not consider IPv6 tunneling when defining security policy, unauthorized traffic could possibly traverse the firewall in tunnels. This is similar to the issue with Instant Messaging (IM) and file sharing applications using TCP port 80 out of organizations with IPv4.
- Many studies of the transition points out that automatic tunneling mechanism are susceptible to packet forgery and DoS attacks. These risks are the same as in IPv4, but increase the number of paths of exploitation for adversaries.
- Tunneling overlays are considered nonbroadcast multiaccess (NBMA) networks to IPv6 and require the network designer to consider this fact in the network security design. The network designer must consider this when deploying automatic or static tunneling.
- Relay translation technologies introduce automatic tunneling with third parties and additional DoS vectors. These risks do not change from IPv4, but do provide new avenues for exploitation. These avenues can be limited by restricting the routing advertisements of relays to internal or external customers.
- Static[123] IPv6 in IPv4 tunneling is preferred because explicit allows and disallows are in the policy on the edge devices.

[119] RFC 4213 *supra* note 116.
[120] D. Thaler, *IP Tunnel MIB*, RFC 4087 June 2005).
[121] RFC 2893 *supra* note 65 and CONVERY *supra* note 96, at 19.
[122] Dual stack hosts run both the current standard, IPv4 and the next generation Internet layer, IPv6.
[123] Generally refers to elements of the Internet that are fixed and not capable of action or change.

- Translation techniques outlined for IPv6 suffer from similar spoofing and DoS issues as IPv4-only translation technologies.
- IPv6-to-IPv4 translation and relay techniques can defeat active defense traceback efforts hiding the origin of an attack.

2.7. Some differences between the two IP-versions related to jurisdictional questions

The following will – with the above sections as a steppingstone - especially deal with whether the new Internet protocol version, IPv6, allows Nations to hinder packages to its citizens as the present version IPv4 must be regarded not to work so. This latter seemed evidenced by a statement from one of the main architect of the IP/TCP protocol, Vinton Cerf: "From the very beginning, we knew that people would try to control information on the Internet. Happily, the net is not very cooperative and we will not have many (censorship) tools."[124]

As the IP protocols are computer-codes the following discussion evidently to a large degree will have to contain technical aspects of the international computer networks rather than a pure discussion of legal terms and theories related to the Nets' functioning and the protocols functioning under the principles of public international law.

Initially should be remarked that if professor Lawrence Lessig[125] and several others are right that "code is law", and if the TCP/IP-v4 protocol according to the constructors of Internet is the "Constitution of the Internet"[126], and none of the users of the World (governments, international organizations and individuals) since the establishment of the protocols has demanded it changed, one could fairly assert, that this international basic protocol-code for interna-

[124] Vinton Cerf to Reuters, *Experts says France could block most Nazi web sales*, November 6, 2000.

[125] Lawrence Lessig, *Legal Issues in Cyberspace: Hazards on the Information Superhighway: Reading the Constitution in Cyberspace*, 45 Emory.L.J. 869, 899 (1996) and LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999 - ISBN 0-465-03913-8).

[126] Or "The cornerstone of the Internet Protocol Suite know as TCP/IP", SILVANO *supra* note 59, at 15-16.

tional computer network, which Lessig describe as law, has become customary international law,[127] which then can be advanced before the International court of Justice in Hague.
If so, then a principal question will be, whether a Nation under public international law can use the Internet Protocol as a mean for national legislation – and under what conditions? This will partly be dealt with in the following subsection 2.7.2.

2.7.1. From a technical point of view

From a technically point of view, if IPv4 is customary international law then every node in the computer network has to comply with it. On the other hand this does not imply that the new version IPv6 cannot be used as an alternative, but only, that IPv6 can only be a service besides of IPv4 - until the international community decides to give up IPv4. The latter means, that computer technicians (including the ISO and ISOC/IETF) cannot change or remove the IPv4 protocol from the public international computer networks – a legal aspect these technicians probably are not aware of.

Thus, a nation has the choice of being a "fully member" of the public international computer networks with acceptance of the present functionality of the IPv4 protocol, or make a subnet (that fulfill its legislative demands) inside its geographical borders with a national gateway to the public international computer networks.

The addressing system of IPv6 changes from that for IPv4 because it includes the ability for one adapter in an IPv6-enabled node to have multiple IPv6 addresses. IPv6 the network designer can assign global unicast addresses only to devices that need to communicate with the global Internet while assigning site-local addresses to devices that need to communicate only within the organization.

IPv6 accommodates local-use unicast addresses, that is, packets with such

[127] SPANG-HANSSEN *supra* note 12 at 341. Pursuant to STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW as amended at the 2000 London conference (International Law Association) nr. 11 page 19 customary law can be created by international organizations. The organs behind the TCP/IP-protocol can fairly be recognized as such international organizations, <http//:www.ila-hq/pdf/CustomaryLaw.pdf> (visited 2003).

addresses can only be routed locally, or within a subnetwork or set of subnetworks of a given subscriber. This should not be against public international law as a State always has had the right to determine whether information can be imported to (or exported from) that State's own citizens. However, it will probably require a great force of people to keep a filter in function.[128]

Furthermore, as it is not practical at the same time to simply replace all IPv4 routers in the Internet with IPv6-routers - and replace all IPv4 addresses with IPv6 addresses - and as the new IPv6 has not been implemented by very many people, experts expect it to take decades - if ever - before the international computer network has changed from IPv4 to IPv6. Thus, there will be a lengthy transition period where the two protocols will coexist. Such a long change-period can allow IPv6 to become customary international law fully or partly. To the extent an IPv6 header works like a comparative IPv4 header the particular IPv6 header-filed can be considered already customary international law.

The IPv4 is making the Internet work much slower than the IPv6 because the first has much more information in its header. To ad more information into the header – or make extension headers – because of legislation wishes from different nations will pursuant to one of the main architect of the original IP/TCP protocol, Vinton Cerf in its utmost consequence imply that "we leave the regulations to anyone in any of 206 countries that can either climb, crawl or get their way into a site to view content, [wherefore you] then have what I characterize as organized chaos."[129]

As one of the main requirements for the IPv6 has been to increase the speed and load on the public computer network, it is critical that routers perform their functions as rapidly as possible. Thus, the following three aspects of the IPv6 design contribute to meet these performance requirements:[130]

[128] SPANG-HANSSEN *supra* note 12, Table 11 at page 96.

[129] SPANG-HANSSEN *supra* note 12 at 531, and Vinton Cerf to Matt Berger, *Yahoo case raises issue of Internet borders*, UpsiteToday, November 3, 2000 <http://www.upside.com> (visited November 2000). Vinton Cerf has called on people "to think more deeply about what they see and hear. That, more than any electronic filter, will build a foundation upon which truth can stand."

[130] STALLINGS-2 *supra* note 66.

- The numbers of fields in the IPv6 packet header are reduced from IPv4.
- The IPv6 packet header is fixed-length whereas the IPv4 header is variable-length. Again, the IPv6 design simplifies processing.
- Packet fragmentation[131] is not permitted by IPv6 routers, although it is in IPv4. In IPv6, fragmentation may only be performed by the source.

Since the unlimited header of the IPv4 slowed the transmission, the IPv6 header was constructed to be more limited, which on the other hand has as a consequence that less control options are in the main IPv6 header. Only if extension IPv6 headers are used by the source will further information and thus control be possible to achieve.

However, a drawback of the change in the header is that is also allows use of extension headers to be used in an attempt to circumvent security policy. Even in IPv4, header manipulation and fragmentation[132] has been used as a technique to bypass access controls on devices such as routers and firewalls. The combination of multiple extension headers and fragmentation in IPv6 creates the potential that the Transport Layer protocol is not included in the first packet of a fragment set, making it difficult to enforce Transport Layer policy on devices that do not do fragment reassembly.[133]

Some IPv6 firewalls understand only a subset of the extension headers in IPv6, and they drop IPv6 traffic that includes these headers. Thus, use of security or control information in headers might hinder deliverance of packets in the future. To the extent it satisfies a nation's legislators, filters can be used. However, surveys show that filters in practice does not work sufficiently and require a lot of daily maintenance.[134]

Legislation through code of the IPv6 would further be opposite another main purpose of the IPv6, namely to make deliverance more certain than in the IPv4 for the requirement of voice-mail and online-TV. If legislation

[131] Packets from one network may have to be broken into smaller pieces to be transmitted on another network, a process known as fragmentation.
[132] IPv4 fragmentation is a technique used to fit the IPv4 datagram into the smallest MTU on the path between end hosts.
[133] CONVERY *supra* note 96.
[134] SPANG-HANSSEN *supra* note 12 at page 97 and Chapter 18.

through code in the nodes on the public international computer network slower or hinder the deliverance, neither voice-mail nor online-TV will be possible to the degree of quality wanted by the users.

Thus, if too many routers or nodes are coded for legislation purposes new features will not be possible and the growth and evolution of the Internet will be stopped to the disadvantage of the citizens in the nations of the World.

2.7.2. From a legislation point of view

The new IPv6 protocol does not to any further extent than the IPv4 seem to help any jurisdictional purposes.

There are no new features in the header of the new IPv6 that helps to decide where the packet comes from or to stop a packet to entering the pipelines of a certain country.

The various tunneling mechanisms offer the ability for a cybernaut with either IPv4 or IPv6 connectivity to send traffic to the other version of IP while masking the true source. As an example, adversaries can use 6to4 relay routers to inject traffic into an IPv6 network with very little ability to trace back to the true source. The IPv4-compatible IPv6 address supports a technique known as automatic tunneling.[135] For each globally unique IPv4-address there exists a mapping to a 6to4 IPv6 prefix.

Subnets[136] in IP seems to ruin the scheme for jurisdictional purposes as the subnet does not have to be in a single Nation, but can belong to a company that is having offices around the world.

Domain names in the new protocol do neither help. National level names still does not have to have any connection to where the computer or user is placed in the world. The new protocol will have more domain names than there exists people, but that does not mean that every person will get a domain name particular related to that person, but rather that each user and

[135] Pekka Savola, *Migration and Co-existence of IPv4 and IPv6 in Residential Networks*, CSC/FUNET, at <http://staff.csc.fi/~psavola/residential.html> (visited October 2005) [hereinafter SAVOLA] and RFC 3964 *supra* note 103 and STALLINGS-2 *supra* note 66.

[136] Subnet - a portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons.

laptop (both of which are not stationary[137]) will have the possibility to have at least one domain name. But a person/user can have more than one IP-address and use different access providers and thus hide with different access-providers from different countries. IPv6 allows a subscriber to use multiple access providers, which might make it harder for States to trace and censure a certain cybernaut's telecommunications.

One cannot protect itself if the router or the receiver gateway only reads part of the headers and skip information in IPv6 extension headers or IPv4 headers.

Internet Layer and Transport Layer spoofing that give a cybernaut the ability to modify their source IP address and the ports they are communicating so to appear as though traffic initiated from another location or another application is not changed in reality between the versions of the IP protocols.[138]

Nothing in the IP protocol stack limits the set of hosts that can establish connectivity to another host on an IP network.

The new IPv6 protocol gives a few possibilities in its new header to make determination of the sender. However, it will take more than 28 years of constant scanning to find the sender (first active host), assuming the first success occurs after iterating through 50 percent of the first 1.8 quadrillion addresses.[139]

Thus it seems that the new IP protocol still does not support Nations government's wish for jurisdictional certainty for legislation and enforcement purposes.

Therefore, countries must give up the idea to have jurisdictional certainty on the Internet. Thus, new parameters must be made in public international

[137] Mobile IP Version 6 (MIPv6) will probably make it even harder to fit a cybernaut into a specific jurisdiction as mobile suppliers offer roaming. See further, C. Perkins (Ed.), *IP Mobility Support*, RFC 2002 (October 1996) & D Johnson, C Perkins, J Arkko, *Mobility Support in IPv6* draft-ietf-mobileip-ipv6-24.txt (June 30, 2003), at <http://www.merit.edu/internet/documents/ietf/59cdrom/proceedings/I-D/draft-ietf-mobileip-ipv6-24.txt> (visited October 2005) and H. Levkowetz & S. Vaarala, *Mobile IP Traversal of Network Address Translation (NAT) Devices*, RFC 3519 (May 2003).

[138] CONVERY *supra* note 96.

[139] *Id.*

law to allow a Nation to legislate and enforce purely online activities.

Requirements in public international law for jurisdiction are closeness and reasonableness. This means that the system in the two IP protocols that to a large extent makes the route from source to destination uncertain does not fulfill the requirements of public international law.

2.8. Final remarks

As it is evident there will be a long transformation period from IPv4 to IPv6 – if IPv4 is ever fully given up – the purpose of making the header of IPv6 "lighter" (to speed up deliverance) will not help for a long time.

The IPv6 does provide new services to the users, as well as powerful capabilities of introducing new ones: end-to-end transparency, autoconfiguration, global addressing and more. The best approach depends heavily on the circumstances.[140] At the same time IPv6 has both benefits and drawbacks from a security standpoint,[141] which means that the IP protocols cannot secure a computer-code provided system of jurisdictions similar and equal to the jurisdictional borders drawn on geographical map.

A conclusion from the previous section seems to be that on one hand is the code of IPv4 – and thus parts of the new IPv6 - protocol customary international law, but on the other hand does the overall technical requirements to these two protocols imply that national legislators cannot use these protocols for legislation purposes as this will destroy the principal wishes of the functionality of the public international computer network.

In the way the IP protocol has been made, features related to jurisdiction and border control can only be implemented at higher levels of the layers in table 2.6 above, namely Process/Application-Layer. This requires that software must be installed on nearly every computer in the world or region, which is an impossible task, especially remembering that the computer technology changes drastic every six-nine month. At the same time, use of extension headers in IPv6 – which is the only way to obtain some kind of location of the user - will slow down the functioning of the Net, which is exactly the

[140] SAVOLA *supra* note 135 and RFC 3964 *supra* note 103.
[141] CONVERY *supra* note 96, at 25.

opposite of the purpose of introducing a new version of the Internet Protocol.

Thus, legislators must find other ways to legislate than software coding on devices on the public international computer networks. They can choose to legislate on the hardware (nodes) inside their own country, but this will on the other hand prevent them from being a "fully member" of the public international computer network with the thereof following advantages, and thus not offer "pipelines" for the public international computer network.

One of the inventors of the TCP/IP protocol stated to the French Yahoo case as to the court requiring filtering "in" the net that "if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning."[142]

[142] SPANG-HANSSEN *supra* note 12 at 118, and Vinton Cerf, November 24, 2000 to *Top Internet advisor criticizes French Yahoo! Decision*, Agence France Press, 2000 WL 24767154 (Westlaw database AGFRP).

CHAPTER 3

Cyberspace & Universal respectively Global Jurisdiction

By Henrik Spang-Hanssen[1]

3.1. Introduction

This chapter will deal with Public International Law and Jurisdiction in relation to Cyberspace.

It is my main view that when discussing the Cyberspace and international public computer network (including the Internet) one should only deal with issues that are special for this media and thus require special handling; whereas the Internet in all other regards should be treated as any other old media, thus using old legislation to solve a certain issue. The main task is thus to find the issues that are special for the international public computer network. The significant new thing about the Internet or international public computer networks is that what before had to be "transported" by use of tangible effects in the brick and mortal world now can be "transmitted" with electronic bits via computer network.

In the following, it will be presumed that the issue is "*pure online*", that is, no physical shipment or tangible things are involved, and at least one user is a foreigner, which is a non-resident or a non-national. Thus, the pre-condition is "pure online" cases with an alien as a defendant with only bit-transmission

[1] I'll like to thank Professor Jiri Toman, Institute of International and Comparative Law, School of Law for comments to this chapter.

as link or connection to the forum State.[2]

3.2. Public International Computer Networks

A major contributor to the Internet's success is the fact that there is no single, centralized point of control or promulgator of policy for the entire network. This allows individual constituents of the network to tailor their own networks, environments and policies to suit their own needs. The individual constituents must cooperate only to the degree necessary to ensure that they interoperate.

The Internet was built on the request that nobody should be able to hinder telecommunication from end user A to end user B. Thus, the inventors of the main protocol for the Internet wanted to make a borderless and international public computer network where people could get access to information on foreign computers and thus exchange point of views. Thus, this computer network was not made to belong to any special State or group of nations, but was intended to belong to the whole world.

3.2.1. Technically

The Internet is not an application but a data delivery service. "Data" is not in itself a service: it is a way of sending the information contained in an application. To a telecommunications transmission technology a signal may be a stream of bits, but to a user it is a telephone call, a webpage, a music program, or a television program. Thus, data may be carried over terrestrial or satellite-based telephone networks, over public or private terrestrial data networks, or over satellites.

Technically the Internet is analogous to an international system of roads and highways, where the national borders only are like street bumps. Its

[2] The non-geographic character of the net makes it very difficult to apply current, territorially-based rules to activities online… Local sovereigns may have a monopoly on the lawful use of physical force, but they cannot control online actions whose physical location is irrelevant or cannot even be established, David Johnson and David Post, *And How Shall the Internet be Governed*, CYBERSPACE LAW INSTITUTE, at <http://www.cli.org/emdraft.html> (visited December 2005).

backbone - the superhighways of the Internet - carries large amounts of information over long distances and there are interchanges on the backbone at network access points (NAP's) and metropolitan area exchanges (MAE's). The "regional" highways is provided by large Internet Service Providers (ISP's) and local ISP's provide "local streets" to the single user's computer or a company's network (a Intranet[3]).

The communication is achieved by having the corresponding - or "peer" - layers in two systems communicate. The peer layers communicate by means of formatted blocks of data that obey a set of rules or conventions known as a protocol.

The Internet's primarily protocols are the Internet Protocol (IP) and Transmission Control Protocol (TCP) (together usually referred to as TCP/IP), which are public protocols that allows for communication between different vendors systems, wherefore the public international computer networks are defined as being "open".

The IP provides multiple routes from one point - "node"[4] - to another with an automatic system, which simply reroutes communication if one part has heavy traffic or is damaged. Every communication is broken into packets by the TCP, so each packet contains the addresses of the sending and receiving computers along with the information to be communicated. The IP is responsible for routing the packets to their destination. Each packet may take a different route across the Internet - and packets may be broken up into fragments. Routers look at the destination address and forward the packet to the next router. The IP does not guarantee the delivery of every packet. On the destination computer, TCP joins the packets into the complete communication and may have to reassemble fragmented packets. TCP may have to request retransmission of missing packets.

Web browsers and Web servers communicate using the TCP/IP. The Web browser sends a request to the Web server, which request includes a portion

[3] Intranet – a private network, within a company or organization, that serves shared applications intended for internal use only – although some may be found on the public Internet.

[4] A node that forwards IP packets (= datagrams) not explicitly addressed to itself. On further, see Hans-Peter Dommel, *Routers and Switches*, in HANDBOOK OF INFORMATION SECURITY (Hossein Bidgoli Ed., 2006, Wiley – ISBN0-471-64833-7).

of the URL for the requested Web page and the version of the HTTP protocol[5] being used. The Web server responds to the request by sending the contents of the requested Web page to the computer on which the Web browser resides. Initially, the Web browser establishes a connection with a Web server through a network before it can obtain the file from the Web server. Typically, this connection is established on the Internet via the TCP/IP connection. To establish a TCP/IP connection, the transport-layer protocol software initiates a request to connect to a special protocol port[6] of the Web server. If the address of the Web server is specified as an IP address in the URL for the requested page, then the computer running the Web browser initiates a request to resolve the domain name into an IP machine address name. Once the TCP connection is made, the Web browser can send repeated Web page requests to the same server without making a new connection.

3.2.2. Public International Law

Public international law[7] is the sum total of legal norms governing rights and duties of the collectivities of the ruling classes - civilized participants in international intercourse in war and peace[8] - without which it would be virtu-

[5] Hypertext transfer protocol - an application layer network protocol built on top of TCP. HTTP's primary function is to establish a connection with a Web server and transmit HTML pages to the client browser.

[6] The port is simply a designator of one of multiple message streams associated with a process. A port address designates a full duplex message stream, Vinton G. Cerf & Robert E Kahn, *A Protocol for Packet Network Intercommunication*, IEEE Transactions on Communications, May 1979, Vol. Com-22, Number 5 page 637, 641, The IEEE Communications Society.

[7] As the International Court of Justice, the European Court of Justice applies public international law, see *Opel Austria GmbH v. Council of the European Union* (E.C.J. T-115/94 1997), 1997 E.C.R. II-39 no. 90 (customary international law whose existence is recognized by the International Court of Justice is binding on the Community), *Ahlstrom Osakeyhtio v Commission of the European Communities* (E.C.J. C89/85 1988), [1988] 4 C.M.L.R. 901, 1988 E.C.R. 5193 no. 22-23 (Commissions decision is not contrary to the rules of public international law), and *Ahlstrom Osakeyhtio v Commission of the European Communities* (E.C.J. C89/85 1993), 1993 E.C.R I-1307 no. 30.

[8] HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION - POSSIBILITIES OF DIVIDING CYBERSPACE INTO JURISDICTIONS WITH HELP OF FILTERS AND FIREWALL SOFTWARE 300 (DJØF Publishing, Copenhagen, 2004 - ISBN 87-574-0890-

ally impossible for the participants to have steady and frequent intercourse.[9] It is not rules, but a normative system that operates in a horizontal legal order.[10] Public international law is a process, a system of authoritative decision-making.[11] It deals with the conduct of nation-states and their relations with other states, and to some extent also with their relations with individuals, business organizations, and other legal entities. In its conceptions, its specific norms and standards, and largely in practice, international law functions between states, as represented by their governments.

Traditionally international public law has been said to govern only relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims.[12] There is no central legislature with general law-making authority and there is no executive institution to enforce law.

It is to be distinguished from Private International Law or Conflicts of Law, which cover a certain State's rules on judicial jurisdiction and competence, foreign judgments and choice of law.[13] Private International Law is

1) [hereinafter SPANG-HANSSEN-2]. Public international law is a "law of the limits" (Grenzrecht), Footnote 78 in Catherine Kessedjian, *Report on International Jurisdiction and Foreign Judgments in Civil and Commercial Mattes*, Hague Conference on Private International Law - Enforcement of Judgments - Prel. Doc. No 7 - Revised Translation of October 1997, at <ftp://ftp.hcch.net/doc /jdgm_pd7.doc> (visited November 2003).

[9] I.A. SHEARER, STARKE'S INTERNATIONAL LAW 14 (11th Edition, Butterworth).

[10] ROSALYN HIGGINS , PROBLEMS & PROCESS – INTERNATIONAL LAW AND HOW WE USE IT 1 (Clarendon Press, Oxford 1994 – ISBN 0-19-876410-3), Rosalyn Higgins , *International Law and the Avoidance, Containment and Resolution of Disputes – General Course on Public International Law*, RECUEIL DES COURS, Vol. 230 (1991-V) page 23.

[11] *Id*. at 267.

[12] Introduction note to Part I, Chapter 1 of Restatement (Third) of Foreign Relation Law [hereinafter REST-Foreign]. Restrictions upon the independence of States cannot therefore be presumed. *S.S. Lotus* (France v. Turkey) 1927 P.C.I.J. (Ser. A) No. 10 para. 18. Also at <www.geocities.com/hssph/Lotus.doc>.

[13] Municipal law governs the domestic aspects of government and deals with issues between individuals, and between individuals and the administrative apparatus, MAL-

law directed to resolving controversies between private persons, natural as well as juridical, primarily in domestic litigation, arising out of situations having a significant relationship to more than one state.

Increasingly, public international law impinges on private international activity, for example, the law of jurisdiction and judgments and the law protecting persons.[14] Public international law is as comprehensive and as sophisticated as the most advanced system of internal law. As any law, international law is not "complete".[15]

However, increasingly international relations develop on all levels, including a transnational society represented by the increasing volume and scope of international co-operation in matters of common concern. An important portion of these transnational relations is carried and promoted by virtually independent semi-public and private groups dealing directly with each other. It is this interplay that determines the structure of public international law. The reordering of international law and an understanding of its new dimensions should proceed from five different perspectives:[16]

- the widening of the scope of public international law through inclu-

COLM N. SHAW, INTERNATIONAL LAW 82 & 100 (4th Edition, Cambridge University Press)[hereinafter SHAW], at 100; IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW at chapter 2 (6th Edition, Clarendon Press, Oxford) [hereinafter BROWNLIE]. The International Court of Justice in the *Barcelona Traction, Light, and Power Co, Limited* (Belgium v. Spain) (Second Phase) of February 5, 1970, 1970 I.C.J. 3, referred to the rules generally accepted by municipal legal systems, not the municipal law of a particular state.

[14] Comments to § 101, REST-Foreign *supra* note 12. "One of the challenges of present-day international law is to provide for stability of international relations and effective international intercourse while at the same time guaranteeing respect for human rights. The difficult task that international law today faces is to provide that stability in international relations by a means other than the impunity of those responsible for major human rights violations," Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal in *Case concerning the Arrest Warrant of 11 April 2000* (Democratic Republic of the Congo v. Belgium) of 14 February 2002, 2002 ICJ 121.

[15] SHABTAI ROSENNE, THE PERPLEXITIES OF MODERN INTERNATIONAL LAW 450 (2004, Martinus Nijhoff Publishers – ISBN 9004136924).

[16] WOLFGANG FRIEDMANN, THE CHANGING STRUCTURE OF INTERNATIONAL LAW 37-39 & 70-71 (Stevens & Sons, 1964).

sion of new subject-matters formerly outside its sphere[17]

- the inclusion, as participants and subjects of international law, of public international organizations and to a less definite extent, of private corporations and individuals;
- the " horizontal" extension of international law, particularly through the accession of non-Western groups of states to the legal family of nations;
- the impact of political, social and economic principles of organization on the universality of public international law, particularly at a time when its scope and subject-matter are expanding;
- the role and variety of international organization in the implementation of the new tasks of international law.

As for public international computer network who's vital protocols are build by transnational scientists to be open source ("freeware") and nearly in all respects are managed by non-governmental organizations or groups, it might not be inappropriate to suggest that jurisdiction over "pure online" incidents will have to vary from the previous norms.

3.2.3. When is a State allowed to legislate and enforce?

No laws of no nation can justify extend beyond its own territories, except so far as regards its own citizens. They can have no force to control the sovereignty or rights of any other nation, within its own jurisdiction.[18]

[17] Now President of the International Court of Justice Rosalyn Higgins has stated: There was a time when international law was perceived as consisting of a manageable corpus of rules over a finite and ascertainable subject matter, relevant in the relations of States with each other. Today the corpus is vast, the subject matter apparently expanding indefinitely, Rosalyn Higgins, *Respecting Sovereign States and Running a Tight Courtroom*, 50 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 121, 122 (2001)(Publisher: British Institute of International and Comparative Law, Oxford University Press).

[18] Justice Story in *The Apollon*, 22 U.S. 362, 370 (U.S. 1824). In Brief of Amicus Curiae the European Commission in *Soda v. Alvarez-Machain* [hereinafter BRIEF OF AMICUS IN *Soda*] argued that United States courts should rigorously apply international law to determine the conduct that gives rise to a violation of the law of nations. "In order to respect the authority of States and organizations, like the European Community, exercising their authority to regulate activities occurring on their own territory,…and hence

Jurisdiction in public international law is usually divided into the following categories:

- **Nationality principle** - confers jurisdiction over nationals of the State concerned. Can be divided into
  - **Active personality principle** - based on the nationality of the suspect. International law accepts jurisdiction over a state's owns citizens based on nationally, or the links between the individual and the state
  - **Passive personality principle** or **Passive nationality principle** - based on nationality of the victim, not the nationality of the offender (controversial)
- **Territoriality principle** confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place.[19] Can be divided into
  - **Subjective territoriality principle** - permits a State to deal with acts which originated within its territory, but was completed or consummated abroad
  - **Objective territoriality principle** – permits a State to deal with acts which originated abroad but which, at least in part, were
    - the "effect doctrine" - consummated or completed within their territory –; or

to preserve harmonious international relations, States must respect the limits imposed by international law on the authority of any individual State to apply its laws beyond its own territory," Brief of Amicus Curiae the European Commission in Support of Neither Party of January 23, 2004 on Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit in *Soda v. Alvarez-Machain et. al.*, 2004 WL 177036 (U.S.) *2 & *3.

[19] The territorial principle is sometimes expressed by saying that a State has jurisdiction over crimes committed on its territory; but this prejudges the guilt of the accused. It would be more accurate to say that a State has jurisdiction over crimes alleged to have been committed on its territory. As soon as the prosecution concedes that the crime was not committed on the State's territory, the court no longer has jurisdiction under the territorial principle, and, unless it can establish jurisdiction under some other principle, it must stop the trial and release the accused, Michael Akehurst, *Jurisdiction in International Law*, 46 BRIT.Y.INT'L (1972-73) 145, 152 note 1[hereinafter AKEHURST].

- the protective theory - producing gravely harmful consequences to the social or economic order inside their territory.

  The protective theory covers a variety of political offences and is not necessarily confined to political acts. The principle is well established and seems justifiable because it protect a state's vital interests. However, it can easily be abused. The decisive is the importance of the offence, which standard is supplied solely by international law.

There exist no treaties, which require a freedom of speech combined with a right to cross-border telecommunication. However, there exist some international declarations that suggest such a regime. For example the Universal Declaration of Human Rights Article 19 declares:[20] "Everyone has the right to freedom of opinion and expression: this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Furthermore, there exists the International Covenant on Civil and Political Rights that states in Article 19:[21] "(1) Everyone shall have the right to hold opinions without interference. (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. (3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

However, this declaration does not mean under international law that free

[20] Adopted by UN General Assembly Resolution 217A (III) of 10 December 1948.

[21] Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976, U.N.T.S. No. 14668, vol. 999 (1976), p. 171.

speech cannot be limited by a nation through legislation.[22] Thus, under public international law nations are to a certain degree allowed to make limits in people's right to publish their opinions, especially if it is related to national security issues, or culture and religious issues, which are often mentioned in a nation's constitution

On the other hand as for free speech and international public law, there exists no international law stating a nation's citizen has to cut off content that is legal in at least one foreign nation besides the citizens own nation - and thus probably acceptable to the U.N. Declaration of Human Rights on free speech.

Pursuant to what seems to be an ever-changing technology on the Internet is it very difficult – if not impossible - to govern the Internet and its users. The Secretary-General of the United Nations stated in 2003, "few manifestations of the power of human creativity have so extensively and so quickly transformed society as the rise of the Internet over the past decade. Dramatic as the changes may be, the process of assimilating and learning from them has only just begun."[23] U.S. Supreme Court Justice Souter has remarked that "we should be shy about saying the final word today about what will be accepted as reasonable tomorrow…In my own ignorance I have to accept the real possibility that…if we had to decide today…just what the First Amendment should mean in cyberspace…we would get it fundamentally wrong."[24]

International public law on jurisdiction to prescribe in relation to international computer network can be summoned up as in the below table as for Pure Online cross-border & the Nationality and Territorial Principles. It should be added to the table that the Subjective Territoriality Principle allows State D to prescribe in all of the fields, whereas the Active Personality Principle allows the State of nationality or residency of the suspect to prescribe in

[22] Confer Article 19(3) of UN International Covenant on Civil and Political Rights, Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976.

[23] Foreword to E-Commerce and Development Report 2003, United Nations, UNCTAD/SDTE/ECB/2003/1 at <http://www.unctad.org/en/docs/sdteecb20031overview_en.pdf >.

[24] *Denver Area Educational Telecommunications Consortium, Inc. v FCC*, 518 U.S. 727, 777 (U.S. 1996).

all of the fields.[25]

	Made online from State D by national of state A	**Made online from State D by national of State C, but citizen of A**	**Made online from State D by national of State B**
Uploaded in State E	International Law involved State E regarded as sender or receiver state?	International Law involved State E regarded as sender or receiver state?	International Law involved State E regarded as sender or receiver state?
Received in State B	International Law involved Objective[26] and Passive[27] personality (controversial) principles allow State B to prescribe?	International Law involved Objective and Passive personality (controversial) principles allow State B to prescribe?	International Law involved

Table 3.1: Jurisdiction to prescribe

This implies for online communication that it has to meet the requirements of the legislation in:[28]

- The State from where the original electronic communication ("bits-transfer") was prepared
- The State where the communication is uploaded
- The State of the communicator's "nationality," that is, for a private owned communication firm where the owner is born, or a corporate is incorporated
- The State where the communicator is a "citizen," that is, for a private

[25] See further SPANG-HANSSEN-2 *supra* note 8, at 300.

[26] The Objective Territoriality Principle permits a State to deal with acts which originated abroad but which, at least in part, were (i) consummated or completed within their territory – the "Effect Doctrine"; or (ii) producing gravely harmful consequences to the social or economic order inside their territory - the "Protective Theory".

[27] The Passive personality principle or passive nationality principle - based on nationality of the victim, not the nationality of the offender.

[28] SPANG-HANSSEN-2 *supra* note 8, at 345.

owned communication firm where the owner living or a corporate is having headquarter

From the receiver site's perspective,[29] it should initially be noted that as the Passive personality principle generally is rejected by the international society, the communicator out of this principle does not have to follow the legislation (statutes or case law) in the state of which the receiver is a nationality. However, the online communicator might have to meet the requirement pursuant to the Objective territoriality principle that permits a State to deal with acts which originated abroad but which, at least in part, were

- consummated or completed within their territory (the "effect doctrine")[30]; or
- producing gravely harmful consequences to the social or economic order inside their territory (the protective theory).

Generally, determining the source of a transmission on the Internet or the location of its reception is a tenuous exercise.[31]

The above mean that a State cannot interfere with what is going on the Internet or on the international network's "pipe-lines" through which the electronic bits of the telecommunication is transmitted. Thus, some international entity is necessary to govern the international networks of computers.

If the above mentioned does not allow to prescribe, a State cannot pursuant to international law make any ruling over telecommunication in the sphere

[29] *Id.* 346.

[30] The use of a trade mark on the Internet, uploaded on a website outside of Australia, without more, is not a use by the website proprietor of the mark in each jurisdiction where the mark is downloaded. However…if there is evidence that the use was specifically intended to be made in, or directed or targeted at, a particular jurisdiction then there is likely to be a use in that jurisdiction when the mark is downloaded. Of course, once the website intends to make and makes a specific use of the mark in relation to a particular person or persons in a jurisdiction there will be little difficulty in concluding that the website proprietor used the mark in that jurisdiction when the mark is downloaded, *Ward Group v. Brodie & Stone*, 143 FCR 479, 491, [2005] FCA 471 (Federal Court of Australia, Victoria Dist., April 2005).

[31] WORLD INTELLECTUAL PROPERTY ORGANIZATION, INTELLECTUAL PROPERTY ON THE INTERNET: A SURVEY OF ISSUES 131, (December 2002 – Doc. WIPO/Int/02) at <http://ecommerce.wipo.int/survey/pdf/survey.pdf> (visited 2003).

called the Internet, which is often illustrated as a cloud in an effort to demonstrate that the information is somewhere in the network on a computer or a fortuitous proxy-server and accessible for everyone from everywhere.

The latter clearly imply that each State's legislators and enforcement has to take great consideration to other State's interests, which always has been the basis for public international law.[32]

Thus, it follows that as telecommunication in form of exchange of ideas and information is done on the public international networks and the exchange is cross-border state lines no single nation can longer by legislation decide what content is legal. Rather, a State can only decide what content its own citizens legally should be allowed to receive through their own "earth station" (laptop, mobile phone, flat screen), whereas the public network cannot be legislated as it is under the "control" of public international law, because the international society does not allow a State to make legislation that lower the functionality of the IP-protocol and thus the packet-delivery of information on the Internet.

At the same time, the Internet has created new problems for communicators as they - opposite the situation in the brick and mortar world - now can expect their communication to become available everywhere and to everyone unless they do something that hinder some people access to their communication or use one-to-one communication like e-mail. If they do not hinder access they can expect liability claims from persons around the whole world that might have been hurt, because the receiver comes from a different culture, religions etc. Thus, the communicator's free speech rights in his own nation might not protect him, if the receiver is outside the communicator's nation and that nation's legislation support remedies or criminal prosecution.

Thus, under public international law most Internet-telecommunication are not under any control of any fortuitous State as in practice most of the information on the Internet is placed on serves outside the State in question.

[32] However, in practice legislators seem to have forgotten this, compare for example Belarus' move to limit online dating by passing a legislation in December 2005 to crack down on Internet dating and online spouse searches, *Belarus Moves to Limit Online Dating*, 14 December 2005, ASSOCIATED PRESS <www.forbes.com/work/feeds/ap/2005/12/14/ap2391504.html> (visited December 2005).

3.2.4. Public Computer Network

If professor Lawrence Lessig[33] and several others are right that ”code is law”, and if the TCP/IP-protocol according to the constructors of Internet is the “Constitution of the Internet”, and none of the users of the World (governments, international organizations and individuals) since the establishment of the protocols has demanded it changed, one can fairly assert, that this international basic protocol-code for international computer network, which Lessig describe as law, has become customary international law,[34] which then can be advanced before and used by the International court of Justice in Hague.[35]

> Some libertarian users see the practice of issuing a Request for Comment (RFC) as a source of “customary” cyberspace law.[36] RFCs37 are editorial managed and publicized by the nonprofit, nongovernmental, international Internet Society (ISOC)[38].

At this place should be mentioned that satellites as for the copper-lines only

[33] Lawrence Lessig, *Legal Issues in Cyberspace: Hazards on the Information Superhighway: Reading the Constitution in Cyberspace*, 45 Emory.L.J. 869, 899 (1996) and LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999 - ISBN 0-465-03913-8).

[34] Pursuant to STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW as amended at the 2000 London conference (International Law Association) no. 11 page 19 customary law can be influenced or maybe even created by international organizations (“The practice of intergovernmental organizations in their own right is a form of "State practice"“), confer page 3 no. 3, page 9 no. b(2) and footnote 44. The organs behind the TCP/IP-protocol can fairly be recognized as such international organizations, <http//:www.ila-hq/pdf/CustomaryLaw.pdf>.

[35] SPANG-HANSSEN-2 *supra* note 8, at 341.

[36] Elisabeth Longworth, *The Possibilities for a Legal Framework for Cyberspace, in* THE INTERNATIONAL DIMENSION OF CYBERSPACE LAW 30 (Law of Cyberspace Series Vol. 1, Ashgate Publishing 2000 – ISBN 0-7546-2146-4).

[37] Request for Comments (RFC) website is <http://www.ietf.org/rfc.html> (visited October 2005). On the process, see R. Hovey, *The Organizations Involved in the IETF Standards Process*, RFC 2028 (October 1996) & RFC Editor et al., *30 Years of RFCs*, RFC 2555 (April 1999).

[38] <http://www.isoc.org>.

are part of the "pipe" lines for the international public networks and that a State is not allowed to hinder or interfere with data-delivery designated between two foreign States by passing another State's territory including airspace.

A State under public international law has the right to make legislation over or totally forbid Earth stations in its territory to communicate with satellites. Under international law the territory include the air space above, but there is no definite km-limit. On the other hand, public international law does not allow a State to legislate or make enforcement on satellites and the telecommunication that is offered by a certain satellite if the satellite is not in a to narrow distance from the Earth.[39] It should be noted, the State in which the owner of a satellite is located or incorporated of cause can give binding orders to that owner. Except for satellites in the Clarke Orbit,[40] which is govern internationally by the ITU,[41] anyone can launce a satellite into orbit and offer telecommunication including the information that can be achieved from the international computer networks.

Thus, under public international law most Internet-telecommunication are not under any control of any fortuitous State as in practice most of the information is only in "transit" through the "pipe-line" of that state in form of a bit send from a foreign country A to country B.

The Internet is as mentioned above a web of networks of computers around the world. The first computer network was involving servers placed in United States, Norway and England.[42] A Working Group under the Interna-

[39] BROWNLIE *supra* note 13, at 105, 255-259, OPPENHEIM 'S INTERNATIONAL LAW 479, 650, 662, 826-845 (London and New York: Longman 9th Ed., paperback edition 1996))[hereinafter OPPENHEIM], and D.J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 244 (5th Edition, Sweet & Maxwell, ISBN 0-421-53470-2Hb).

[40] Or the Geosynchronous Orbit. Satellites in this orbit (GSOs) are launched into a band 35,786 (22,300 miles) in altitude above Equator where it moves in consonance with the terrestrial globe and therefore is constantly over the same point. Three GSO-satellites can cover the total surface of the Earth. However, a GSO satellite cannot see any areas with latitude more than 77° north or south.

[41] Because the Clarke Orbit is only of 265,000 km in range is requires an administration of this "limited natural resource" like the radio frequencies also administrated by ITU.

[42] *History - ARPAnet 1957 – 1990*, at <http://www.jmusheneaux.com/21bb.htm> (visited December 21, 2005); A Note on the Internet page 2, Graduate School of Business,

tional Telecommunications Union (ITU) has defined the Internet as the publicly accessible global packet switched network of networks that are interconnected through the use of the common network protocol IP.[43] It encompasses protocols; names and addresses; facilities; arrangements; and services and applications.

> The Internet was designed without any contemplation of national boundaries. The actual traffic in the Net is totally unbound with respect to geography. The only "passports" on the Internet are IP-addresses, sets of four numbers separated by periods, which have no direct correlation to where a person's computer is located. IP-addresses are intended to be used to keep straight all the data that flows between machines. They are not like phone numbers, with area codes.44
>
> There are still serious questions about whether Geolocation technologies can, in fact, determine locations with any certainty. People using a satellite-based Internet service provider can be anonymous to an ordinary location tracker. Programs like Anonymizer and SafeWeb, which disguise a computer's IP-address, can also fool geolocation systems.45

Another vital aspect of the telecommunication on public international computer networks is the use of the HTTP protocol that was made by an Englishmen working in Switzerland. Berners-Lee, who invented the World Wide Web around 1990, actually dedicated the protocol to the whole world.[46] This

Stanford University 1996, at <www.stanford.edu/group/scip/Afeche-internet.pdf> (visited December 21, 2005).

[43] H. Zhao, *ITU and Internet governance*, 15 December 2004, ITU Council Working Group on the World Summit on the Information Society Geneva 13-14 December 2004, WG-WSIS-7/6 Rev 1 at <www.wgig.org/working-papers.html> (visited March 2005).

[44] Internet protocol architect Vinton Cerf to Lisa Guernsey, *Welcome to the Web. Passport, Please*?, THE NEW YORK TIMES – TECHNOLOGY, March 15, 2001, <http://tech2.nytimes.com/mem/technology/techreview.html?res=9B01E7D71F3AF936A25750C0A9679C8B63> (visited November 27, 2005).

[45] Lisa Guernsey, *id*.

[46] He is now director of the World Wide Web Consortium (W3C), which aim is to ensure the www's interoperability, <http://www.ibiblio.org/pioneers/lee.html> (visited April 2003). See further SPANG-HANSSEN-2 *supra* note 8, at 2 and *American Civil Liberties Union v. Reno*, 929 F.Supp 824, 836 para. 35 and *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 483 and Jeff Groff, who worked with Mr Berners-Lee on the

was made with the purpose to ease the interchange of information from one computer to another thus making it possible to get information from foreign computers or networks. Thus, HTTP, which is the basis for websites, is made with purpose of making telecommunication across borders easy and accessible on an international computer network.

This shows that the inventors of the IP protocol and HTTP wanted to make a borderless and international public computer network where people could get access to information on foreign computers and thus exchange point of views.

In "A Framework for Global Electronic Commerce" was stated: "The Global Information Infrastructure ("GII"), still in the early stages of its development, is already transforming our world.... As the Internet empowers citizens and democratizes societies it is also changing classic business and economic paradigms…One of the principles that the U.S. believes should be the foundation for government policy... [is] guaranteeing open access to networks on a non-discriminatory basis, so that GII users have access to the broadest range of information and services."[47]

Furthermore, "technology will make it increasingly difficult for the states to control the information its people receive…The Goliath of totalitarianism will be brought down by the David of the microchip."[48]

Thus, this computer network was not made to belong to any special State or group of nations, but was intended to belong to the whole world. Thus, the computer network has from the very beginning been an international network.

It should thus with good reason be stated that the Internet should be gov-

early code, has stated that a very simple idea was behind the web in 1991; and now in 2006 the web may be worldwide but it is only just getting started. The original conception was for a medium that people both read and contributed to. New tools such as photo-sharing sites, social networks, blogs, wikis and others are making good on that early promise, Mark Ward, *How the web went world wide*, BBC NEWS 3 August 2006 at <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/5242252.stm> (visited August 2006).

[47] William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 4, 1997) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (visited Nov. 21, 1997).

[48] Ronald Reagan in speech at London's Guildhall (June 14, 1989).

ern by the international society.

It does not belong to any State or group of States in the world. Thus, the Internet is something like the High Sea belonging to the international society of States and under the reign of public international law.

The IP protocols cannot secure a computer-code provided system of jurisdictions similar and equal to the jurisdictional borders drawn on geographical map. On one hand is the code of IPv4 – and thus parts of the new IPv6 - protocol customary law, but on the other hand does the overall technical requirements to these two protocols imply that national legislators cannot use these protocols for legislation purposes as this will destroy the principal wishes of the functionality of the public international computer network.[49]

One of the inventors of the TCP/IP protocol stated to the French Yahoo case as to the court requiring filtering "in" the net that "if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning."[50]

The problem is twofold. Filters can only be installed in the so-called Application layer[51] – not in the Internet-protocol (IP/TCP) – and to function properly all notes on the public computer network must have installed the filter application. However, no one has total control over all the notes.

Therefore, countries must give up the idea to have jurisdictional certainty on the Internet. Thus, new parameters must be made in public international law to allow a Nation to legislate and enforce purely online activities.

Requirements in public international law for jurisdiction are closeness and reasonableness. This means that as the system in the two IP protocols to a large extent makes the route from source to destination uncertain it does not fulfill the requirements of public international law.

[49] Pekka Savola, *Migration and Co-existence of IPv4 and IPv6 in Residential Networks*, CSC/FUNET, at <http://staff.csc.fi/~psavola/residential.html> (visited October 2005) and P. Savola & C. Patel*, Security Considerations for 6to4*, RFC 3964 (December 2004) and Sean Convery & Darrin Miler, *IPv6 and IPv4 Threats Comparison and Best-Practice Evaluation (v1.)* page 25.

[50] SPANG-HANSSEN-2 *supra* note 8, at 118, and Vinton Cerf, November 24, 2000 to *Top Internet advisor criticizes French Yahoo! Decision*, Agence France Press, 2000 WL 24767154 (Westlaw database AGFRP).

[51] See Table 2.6 "ARPA – OSI Layers" in this book chapter 2.

3.3. Jurisdiction

Normally[52] no State is allowed to apply its legislation to foreigners in respect of acts done by them outside the dominions of the sovereign power enacting. That is the rule based on public international law, by which one sovereign power is bound to respect the subjects and the rights of all other sovereign powers outside its own territory.[53] This statement refers not only to legislation - statutes or common law - but also to all judicial and executive acts giving effect to the sovereign's will.[54]

The legally relevant point of contact in the doctrine of international jurisdiction will have to be defined as indicating the State, which has a close – rather than the closest – connection with the facts, a genuine link, and a sufficiently strong interest. Yet not every close contact will be legally acceptable. It should not be at the discretion of States or judges, but by the objective standards of international law. It to a reasonable relation – that is absence of abuse of rights or of arbitrariness[55] - and a policy of tolerance, reasonableness and good faith.[56]

[52] SPANG-HANSSEN-2 *supra* note 8, at 240-242.

[53] Lord Russells of Killowen in 1897 in *The Queen v. Jameson*, [1896] 2 Q.B. 425, 430 (U.K. Queens Bench, 1896), *Lauritzen v. Larsen*, 345 U.S. 571, 578, 582 (U.S. 1953) ([I]t has long been accepted in…jurisprudence that if any construction otherwise be possible, an Act will not be construed as applying to foreigners in respect to acts done by them outside the dominions of the sovereign power enacting. That is a rule based on international law, by which one sovereign power is bound to respect the subjects and the rights of all other sovereign powers outside its own territory….rules designed to foster amicable and workable commercial relations), *Romero v. International Terminal Operating Co*, 358 US. 354, 382, 384 (US 1959), *William Benz v. Compania Naviera Hidalgo, S.A*., 353 US 138, 144, 147 (US 1957), *West India Fruit and Steamship Comp. v. Seafarers International Union of North America, Atlantic & Gulf District*, 130 NLRB 343, 350-364 (National Labor Relations Board, 1961).

[54] F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 4 (1990, Clarendon Press, Oxford) [hereinafter MANN-2].

[55] F.A. MANN, *The Doctrine of Jurisdiction in International Law*, 111 Recueil Des Cours 1, 46-47 (1964-I) [hereinafter MANN-1].

[56] MANN-1 *supra* note 55, at 48, referring to *Lauritzen v Larsen*, 345 US 571, 582 (US 1953): In dealing with international commerce we cannot be unmindful of the necessity for mutual forbearance if retaliations are to be avoided; nor should we forget that

A temporary visitor is subject to local legislation, which regulates conduct within the territory of the State. But the local sovereign has to exclude the temporary visitor's activity abroad. Attempt by a State to subject the foreign transactions of its non-residents citizens to its exchange control regulations would to be improper. Nationality is a wholly inadequate nexus.[57]

As civil jurisdiction[58] is ultimately reinforced by procedures of enforcement involving criminal sanctions, there is in principle no great difference[59] between the problems created by assertion of civil and criminal jurisdiction over aliens.[60]

Criminal jurisdiction is designed to promote security and certainty in international life to prevent friction among nations. To be entitled to assume legislative jurisdiction there must exist a close connection in an international sense between the person, fact or event and the State imposing criminal liability in regard to them. The real problem of international law is to define the circumstances. The limits of a State's criminal jurisdiction should be found in the doctrine of the abuse of rights.[61]

any contact which we hold sufficient to warrant application of our law to a foreign transaction will logically be as strong as warrant for a foreign country to apply its law to an American transaction.

[57] Forum non conveniens is in the US given wide scope, while in England is limited by the requirement that there is another forum where justice can be done at less inconvenience and expense and where the plaintiff is not deprived of a substantial advantage, MANN-2 *supra* note 54, at 6, 8 and 9.

[58] SPANG-HANSSEN-2 *supra* note 8, at 237-239.

[59] BROWNLIE *supra* note 13, at 298. OPPENHEIM *supra* note 39, at 466.-484, 763.

[60] Michael Akehurst finds Brownli's point of view rather extreme, "the rules governing the jurisdiction in civil and in criminal cases are founded in many respects on radically different principles, and…an assumption of jurisdiction over an alien in the one case is not to be made a precedent for a like assumption in the other and…conversely that limitations in criminal cases cannot be cited as authority for the existence of like limitations in civil cases…[T]he only limitation on jurisdiction in civil trials [is] contained in the principle of effectiveness…[W]hen one examines the practices of States [these] claim jurisdiction over all sorts of cases and parties having no real connection with them and that this practice has seldom if ever given rise to diplomatic protests, AKEHURST *supra* note 19, at 170.

[61] SPANG-HANSSEN-2 *supra* note 8, at 237-240 and MANN-1 *supra* note 55, at 82 and 83.

The strictly territorial character for the doctrine of international jurisdictional has been much relaxed by the need to treat reasonable closeness of contract as a substitution for or, to put it at its lowest, a supplementary element in, the commanding position of territorial sovereignty;[62] and nothing indicate in the international field that the rule of the plaintiff having to submit to the defendant's court[63] has been superseded by a rule of plaintiff's very intimate connection with the forum.

Yet, it seems likely that in the modern world the territorial test fails to give compete satisfaction.[64] Perhaps the exercise of a State's civil jurisdiction should presuppose no more than "certain minimum contacts[65] with it such that the maintenance of suit does not offend traditional notions of fair play and substantial justice."[66]

3.3.1. Types of Jurisdiction

Until now analyses on jurisdiction in relation to Cyberspace and public international law has been based on the pattern, what - until the invention of public international computer network – previous reasonably could be used in public international law, namely the categories mentioned above in section 3.2.2.

However, these categories was made before the event of public international computer network on which everything can be accessed from anywhere, and by anybody, and at the same time, or phrased otherwise, information is accessible worldwide for the whole world at the same time, wherefore all (or none) states can claim jurisdiction because information is accessible in every State.

This incontrovertible and indisputable fact requires a whole new jurisdic-

[62] MANN-2 *supra* note 54, at 52.
[63] The maxim "Actor sequitur forum rei".
[64] MANN-1 *supra* note 55, at 74.
[65] "minimum contact" "is a substitute for physical presence," *Burnham v. Superior Court of California*, 495 U.S. 604, 620 (US 1990).
[66] *International Shoe v. State of Washington*, 326 U.S. 310 (US 1945). The Statute for the new International Criminal Court ("ICC") recognizes complicit liability, ICC statute article 25(3).

tional analysis[67] for these new instances of "pure online" acts done by aliens, which is the requirement for the rest of this chapter. The analysis will further be dealt with below in section 3.4.

The following introduce some new terms in relation to analyze of jurisdiction in public international law under the just mentioned requirements. Firstly, introducing a new primary head-grouping into (α) Universal jurisdiction and (β) National jurisdiction. Secondly, introducing a new secondary head-grouping into (a) Global jurisdiction where a State's jurisdictional rules taken on its "wording" reaches all alien cybernauts, (b) Transnational jurisdiction between parties of a treaty, and (c) Restricted jurisdiction where a State has chosen to limit the group of possible defendants to the definition given below.

At the same time should here be pointed out – as mentioned above – that the default or basis rule in public international law is that the alien defendant's home-forum is the basic-jurisdiction.[68] It might be that this basic rule should be even more appropriate in "pure online" cases, because otherwise the alien cybernaut will have to accept too many deviation and departure from this old basic rule whereby the alien defendant can risk being sued in any court in the world, what state of the law has never been accepted by public international law.

There exist several types of jurisdiction that can be used in relation to aliens.

Initially should be remarked that since this chapter is only dealing with "pure online" cases the presumption is that the alien has no physical effects in the forum's territory, wherefore in rem[69] and quasi-in-rem[70] jurisdiction

[67] This might be the same analyze the International Court of Justice will have to do, when considering whether a national jurisdiction rule is too broad in relation to a "pure online" matter.

[68] The maxim "actor sequitur forum rei". This is also the starting point for the E.U. Council Regulation 44/2001 of 22 December 20000 on Jurisdiction article 2(1). See also SPANG-HANSSEN-2 *supra* note 8, at 240-242.

[69] A court's power to adjudicate the rights to a given piece of property, including the power to seize and hold it. A number of countries claim jurisdiction whenever the defendant has assets within the State concerned. In some States (the Netherlands, South Africa, many states in the United States) jurisdiction is limited to the value of the assets; in

has no relevance here.[71]

In some countries, rules on jurisdiction are divided in to two main groupings: Subject Matter Jurisdiction[72] and Personal Matter Jurisdiction; and in countries like the U.S., the court will first and separately deal with the matter of personal jurisdiction. In the following, the term "jurisdiction" will relate to what in the U.S. is called personal jurisdiction, that is, a court's power to bring a person into its adjudicative process.

Another main division of jurisdictional rules is now introduced, see above:

- **Universal jurisdiction** – a court of a nation acts on behalf of the in-

other States (Austria, Belgium, Denmark, Germany, Scotland, Sweden, Japan, parts of Switzerland) it is not so limited. It is obvious that this rule enables a State to exercise jurisdiction over cases and parties having no real connection with that State, but no State seems to have protested that such jurisdiction is contrary to international law, AKEHURST *supra* note 19, at 171-72; L. I. de Winter, *Excessive Jurisdiction in Private International Law*, 17 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 707, 708, 713 (1968). In Germany the defendant's assets include a claim for which the defendant could sue the plaintiff in German court: Henry P. de Vries and Andreas F. Lowenfeld, *Jurisdiction in Personal Actions – A Comparison of Civil Law Views*, 44 IOWA LAW REVIEW 306, 332-39 (1959). In the United States jurisdiction is limited to the value of the assets unless the defendant appears in order to challenge the claim on the merits-but this confronts the defendant with a harsh dilemma, see David F. Cavers, *Contemporary Conflicts Law in American Perspective*, 131 RECUEIL DES COURS 75, 295 (1970-III).

[70] Jurisdiction over a person but based on that person's interest in property located within the court's territory.

[71] It is probably against public international law that the U.S. Anti Cybersquating Protection Act (ACPA), 15 USC § 1125(D) allows in rem jurisdiction for designated types of claims for the court located where a domain name was registered, *see Barcelona.com, Inc. (U.S.) v. Excelentisimo Ayuntamiento de Barcelona* (City Council of Barcelona, Spain), 330 Fed 617 (4th Cir. 2003). The provision has been constitutionally challenged, but challenged has failed by 1st Circuit in *Sallen v. Corinthians Licenciamentos* LTDA, 273 F.3d 14, 60 U.S.P.Q.2d 1941 (1st Cir. 2001); by 2nd Circuit in *Mattel, Inc. v. Barbie-Club.com*, 310 F.3d 293 (2002); by 4th Circuit in *Porsche Cars North America, Inc. v. Porsche.Net*, 302 F.3d 248 (2002), *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214 (2002), Cable *News Network v. CNNews.com*, 56 Fed.Appx. 599 (2003). On The United States Constitution and International Law see for example *Agora*, 98 AM.J.INT'L L. 42, 43, 57, 69, 82, 91 (January 2004).

[72] Jurisdiction over the nature of the case and the type of relief sought; the extent to which a court can rule on the conduct of persons or the status of things.

ternational society pursuant to public international law, see below

- **National jurisdiction** – a court of a nation acts on behalf of its sovereign. It involve two terms: International jurisdiction[73] and Exterritorial jurisdiction,[74] which is formulated by the particular nation itself, wherefore it can be in violation with public international law.[75] It can be divided into the following sub-categories: Global Jurisdiction
    - **Global jurisdiction** - (Worldwide) jurisdiction involving aliens whom can be anywhere in the world (outside the forum state). This kind of jurisdiction can be exercised on basis of:
        - *General jurisdiction* - even if the cause of action is unrelated to the activities at issue, if only the alien defendant's activities in the forum state are "substantial, continuous, and systematic" (and the particular long-arm statute's requirement is fulfilled)[76]

          In U.S. this is a fairly high standard in practice that is very difficult to meet. The U.S. Supreme Court has upheld the use of general juris-

[73] A court's power to hear and determine matters between different countries or persons of different countries.

[74] On U.S. exterritorial reach, see for example *Sterling Drug, Inc. v. Bayer AG*, 14 F.3d 733, 745-6 (2nd Cir. 1994) and *Hartford Fire Insurance Co v. California*, 509 U.S. 764, 798-99 (US 1993).

[75] A court's ability to exercise power beyond its territorial limits (confer long-arm statute [A statute providing for jurisdiction over a nonresident defendant who has had contacts with the territory where the statue is in effect]).

[76] *Helicopteros Nationale de Colombia, S.A. v. Hall*, 466 U.S. 408, 414-416 (U.S. 1984). A Canadian Court used the analysis from the *Panavision* v. *Toeppen*, 141 F.3d 1316,1320 (9th Cir. 1998) to conclude, that there was no general jurisdiction over defendant, *Easthaven Ltd. V. Nutrisystem.com Inc*., 2001 CarswellOnt 2878 (Ontario Superior Court, No. 00-CV-202854, August 2001)

diction only in one case.[77]

- *Specific jurisdiction* - cause of action arise from defendant's minimum contacts with the forum state

In U.S. case law on the issue of specific personal jurisdiction and Internet an alien's activities amount to purposeful availment of the forum state rendering the exercise of personal jurisdiction over the alien pursuant to:[78]

- the sliding scale approach,[79] as articu-

[77] *Perkins v. Benquet Consol. Min. co, 342 U.S. 437* (US 1952). But *see*, *Provident Nat. Bank v. California Federal Sav. & Loan Ass'n.*, 819 F.2d 434 (3rd Cir. 1987).

[78] SPANG-HANSSEN-2 *supra* note 8, at 385-386. *Healthcare Alliance Inc. v. Healthgrades.com, Inc*., 50 Fed.Appx. 339, 2002 WL 31246123 (9th Cir. 2002) (Plaintiff was suing in tort and seems only to claim specific personal jurisdiction, which was allowed), *cert. denied*, 123 S.Ct. 1909 (US April 28, 2003, No. 02-1250). *McBee v. Delica*, 2003 WL 1872907, 2003 U.S. Dist. LEXIS 6123 at *1 (D. Maine, April 14, 2003), which recommended decision of the Magistrate Judge was affirmed by 2003 WL 21553820 (D. Maine, July 9, 203) (Jurisdiction over Japanese defendant, which had no contact to the U.S. but for a website hosted in Japan - and written almost entirely in Japanese - but accessible for U.S. residents, although these could not buy products directly from the website. Instead, they had to place orders directly with defendant's stores in Japan. Defendant had in three cases accepted orders from residents of the U.S. courts forum). *Swarovski Optik North America v. Euro Optics*, 2003 WL 22014581 (D. Rhode Island, August 2003) (No jurisdiction over Pennsylvania defendant, who had no other contacts with court's forum than a website. Only U.S. residents could purchase products from defendant's website, because the online order form only allowed purchasers to choose a U.S. location. The court held that the fact that residents in the court's forum could order products from the website, without more, was insufficient to establish purposeful availment in a case where defendant amongst others sold plaintiff's products – though not authorized by plaintiff – which it obtained form European distributors).

[79] Texas courts apply the approach "in both general jurisdiction and specific jurisdiction cases," *Carrot Bunch Co, Inc. v. Computer Friends, Inc*., 218 F.Supp.2d 820, 825 (N.D.Tex. Aug. 2002).

lated in *Zippo*[80] and *Cybersell*[81] and[82]
- the effects test, endorsed by the Supreme Court in *Calder v. Jones*[83], and adopted by the Ninth Circuit in *Panavision*[84].

- *Transnational jurisdiction* – which exists pursuant to the Treaty against Transnational Organized Crime is present when:[85]
  - The offence is committed in more than one State
  - It is committed in one State but a sub-

[80] *Zippo Manufacturing Comp. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119, 1123-1124 (W.D. Pa. 1997) . See further this book Chapter 4.

[81] *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 417-19 (9th Cir. 1997).

[82] The Zippo model has been adopted by the Fourth Circuit in *Als Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Cir, June 2002) to which *certiorari* was *denied* in 123 S.Ct. 868 (US, January 2003). The Zippo scale has also been positively discussed by other Appeals courts: the Fifth Federal Circuit in *Mink v. AAAA Development LLC*, 190 F.3d 333, 336 (5th Cir. (Tex), 1999), by Six Federal Circuit in *Neogen Corp. v. Neo Gen Screening, Inc.*, 282 F.3d 883, 890 (6th Cir. (Mich) Mar. 2002) and *Bird v. Parsons*, 289 F.3d 865, 875 (6th Cir. (Ohio) May 2002), by Ninth Federal Circuit in *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 418 (9th Cir. (Ariz.) Dec 1997) and by Tenth Federal Circuit in *Soma Medical International v. Standard Chartered Bank*, 196 F.3d 1292, 1296 (10th Cir. (Utah) Dec 1999). The Zippo case has also been cited by the D.C. Federal Circuit in *Gorman v. Ameritrade Holding Corp*., 293 F.3d 506, 513 (D.C.Cir. June 2002).

[83] *Calder v. Jones*, 465 U.S. 783, 788-89 (US 1984).

[84] *Panavision Int'l L.P. v. Toeppen*, 141 F.3d 1316, 1321-22 (9th Cir. 1998). See also, *Denenberg v. Ruder*, 2006 WL 379614 at *4 (D. Nebraska, Feb. 2006)(Whether or not defendant's website aimed at soliciting business in Nebraska was not central to the personal question "in this case" "[b]ecause" defendant purposefully and fraudulently misappropriated copyrighted materials from plaintiff).

[85] Article 3(2) of "Palermo Treaty" or United Nations Convention Against Transnational Organized Crime", A/RES/55/25 at <http://www.unodc.org/unodc/en/crime_cicp_resolutions.html>. As of 23 November 2005: 147 signatories and 114 parties: at <http://www.unodc.org/unodc/en/crime_cicp_signatures_convention.html> (visited November 2005).

stantial part of its preparation, planning, direction or control takes place in another State
- It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
- It is committed in one State but has substantial effects in another State.

- **Restricted jurisdiction** – Jurisdiction that a State through statute or caselaw has limited to cases where the defendant at the time of the act is a residents or national of the forum state, or visitor in the forum state.

The latter is equal to a combination of the active personality principle and the subjective territorial principle. As restricted jurisdiction cannot in the sense of public international law be said to deal with "aliens", which latter is the subject of the rest of this chapter, this kind of jurisdiction will not be further dealt with.

3.3.2. Universal jurisdiction

The Universal Jurisdiction Principle[86] – which is not limited to criminal law[87] - is not linked to the nationality of the suspect or victim or to harm to the forum state's own national interests. When a state asserts universal jurisdiction, it is not prescribing a domestic legal rule that applies worldwide, but it is merely exercising adjudicatory jurisdiction based on a rule of international

[86] SPANG-HANSSEN-2 *supra* note 8, at 252-254. M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical perspectives and contemporary practice*, 42 VA.J.INT'T L. 81 (2001) [hereinafter BASSIOUNI]; Kenneth C. Randall, *Universal Jurisdiction under International Law*, 66 TEX.L.REV. 785 (1988); SHAW *supra* note 13, at 470; ANTONIO CASSESE, INTERNATIONAL LAW 261 (1st Edition, Oxford University Press - ISBN 0-19-829998-2).

[87] Comment b to § 404 of REST-Foreign *supra* note 12.

law and national courts act instead of international organs.[88]

This principle that allows jurisdiction over acts of non-nationals where the circumstances, including nature of the crime, justify the repression of some types of crime as a matter of international public policy.[89]

Commentators disagree on how to ascertain whether universal jurisdiction is well established in customary international law: for some, the acceptance by states that a practice is obligatory (opinio juris) is enough; for others, the consistent practice of states is required.[90] There is no evidence that the application of universal jurisdiction in state practice has arisen to the level of customary international law.[91] Customary international law currently does not provide for the prosecution of "terrorist" acts under the universality principle.[92]

> The European Union remarked in a brief of Amicus Curiae to the U.S. Supreme Court that customary international law is evolutionary in nature, so the norms encompassed by a state's statute will change over time. International

[88] AMNESTY INTERNATIONAL, UNIVERSAL JURISDICTION (2001) (AI Index: IOR 53/003/2001) at <www.amnesty.org> or <www.iccnow.org> [hereinafter AMNESTY], at Chapter One.

[89] BROWNLIE *supra* note 13, at 303; I.A. SHEARER, STARKE'S INTERNATIONAL LAW 212 (11th Ed. Butterworth 1994); REST-Foreign *supra* note 12, at § 404.

[90] THE PRINCETON PRINCIPLES page 40, at <www.princeton.edu/~lapa/unive_jur.pdf> (visited November 2005) [hereinafter THE PRINCETON PRINCIPLES].

[91] BASSIOUNI *supra* note 86, at 148. Otherwise, AMNESTY *supra* note 88, at Chapter One, page 11 (2001) (AI Index: IOR 53/003/2001). See also Bernard H. Oxman, *Arrest Warrant of 11 April 2000*, 96 AM.J.INT'L L. 677, 681 [hereinafter OXMAN] that holds in relation to jus cogens crimes "it would be an extremely formalistic approach to make existence of universal jurisdiction…depends upon the presence of an accused on a state's territory" and *Case concerning the Arrest Warrant of 11 April 2000* (Democratic Republic of the Congo v. Belgium) of 14 February 2002, 2002 ICJ 121.

[92] *United States of America v. Yousef*, 327 F.3d 56, 97 (2nd Cir 2003)(The appeal court held jurisdiction under U.S. law (18 U.S.C. §32) adopted from the Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation – 1993 bombing of World Trade Center in New York).

> law sanctions universal criminal jurisdiction in order to end impunity for violations of the most fundamental norms of international law.[93]

It is important to recall that simply because certain offenses are universally condemned does not mean that a state may exercise universal jurisdiction over them. It is of great concern that particular states can abuse universal jurisdiction to pursue politically motivated prosecutions.[94]

The term "universal jurisdiction" related to Cyberspace cases has been rejected by a number of U.S. Courts.[95]

A considerable number of states have adopted universal jurisdiction - usually with limitations. Most laws claiming jurisdiction under the universality principle – opposite under the passive personality principle[96] - expressly mention some or all of these restrictions.[97] There are various limitations, such as that no other country wishes to exercise a jurisdiction on the territorial principle, or Universal jurisdiction is provided only if the accused is in the territory of a state whose legislation recognizes as a general rule the principle of the prosecution of offences committed abroad by foreigners.[98] In relation to jus cogens crimes "it would be an extremely formalistic approach to make

[93] BRIEF OF AMICUS IN *Soda supra* note 18, at *4 about the U.S. Alien Tort Statute, 28 U.S.C. § 1350s.

[94] THE PRINCETON PRINCIPLES *supra* note 90, at 43. *Attorney General of Israel v. Eichmann,* 36 I.L.R. 5 (Isr. D.C., Jerusalem, 12 Dec. 1961), *aff'd*, 36 I.L.R. 277 (Isr. S. Ct., 29 May 1962), is often cited as representing the exercise of universal jurisdiction by Israel, although many argue that the decision was more fundamentally predicated upon the passive personality doctrine and the protective principle under a unique Israeli statute passed by the Knesset in 1950.

[95] SPANG-HANSSEN-2 *supra* note 8, at footnote 1463 mentions: *Cybersell, Inc. (Arizona) v. Cybersell, Inc. (Florida)*, 130 F.3d 414, 415 & 419 (9th Cir. 1997), *Hearst Corp. v. Goldberger*, 1997 WL 97097 * 1 & *16 & *20 (S.D.N.Y. 1997), *Digital Equipment Corp. v AltaVista Technology, Inc*. 960 F.Supp. 456, 463 (D.Mass. 1997), *Edberg v. Neogen Corp*., 171 F.Supp.2d 104, 114 (D.Conn. 1998), *Hasbro, Inc. v. Clue Computing, Inc*., 994 F.Supp 34, 46 (D.Mass. 1997), *Playboy Enterprise, Inc. V. Chuckleberry Publication, Inc*. (Tattilo), 939 F.Supp 1032, 1039 (S.D.N.Y. 1996).

[96] See *Attorney General of Israel v. Eichmann,* above footnote 94.

[97] AKEHURST *supra* note 19, at 166 footnote 3.

[98] C. Jessup, INTERNATIONAL LAW STUDIES, U.S. NAVAL WAR COLLEGE, VOL. 61, page 305-308 (Naval War College, 1980), and AKEHURST *supra* note 19, at 161.

existence of universal jurisdiction depends upon the presence of an accused on a state's territory."[99]

> In the above mentioned brief of Amicus Curiae the European Union further remarked, that the existence and scope of universal civil jurisdiction is not well established. To the extent that universal civil jurisdiction is recognized, it applies only to a narrow category of cases. Any exercise of universal civil jurisdiction should also be limited in accord with its rationale. Hence, a State should exercise universal civil jurisdiction where that exists under international law, only when the claimant would face a denial of justice in any State that could exercise jurisdiction on a traditional basis, such as territory or nationality.[100]
>
> The U.S. Supreme Court were persuaded that federal courts should not recognize private claims under federal common law for violations of any international law norm with less definite content and acceptance among civilized nations than the historical paradigms familiar when [Alien Tort Statute 28 U.S.C.] § 1350 was enacted. For purposes of civil liability, the torturer has become - like the pirate and slave trader before him - hostis humani generis, an enemy of all mankind. Actionable violations of international law must be of a norm that is specific, universal, and obligatory. And the determination whether a norm is sufficiently definite to support a cause of action should (and, indeed, inevitably must) involve an element of judgment about the practical consequences of making that cause available to litigants in the federal courts.[101]
>
> This requirement of clear definition is not meant to be the only principle limiting the availability of relief in the federal courts for violations of customary international law, though it disposes of this case. For example, the European Commission argues as amicus curiae that basic principles of international law require that before asserting a claim in a foreign forum, the claimant must have exhausted any remedies available in the domestic legal system, and perhaps in other fora such as international claims tribunals.[102] We would certainly consider this requirement in an appropriate case.[103]

[99] OXMAN *supra* note 91, at 681.
[100] BRIEF OF AMICUS IN *Soda supra* note 18, at *5.
[101] *Soda v. Alvarez-Machain et. al.*, 542 U.S. 692, 732, 733 (US June 2004) [hereinafter *Soda*].
[102] BRIEF OF AMICUS IN *Soda supra* note 18, at *24 footnote 54, citing BROWNLIE *supra* note 13, at 472-481.
[103] *Soda supra* note 101, at footnote 21.

> U.S. Justice Breyer remarked in a concurring opinion to the Supreme Court decision:[104] The fact that this procedural consensus exists suggests that recognition of universal jurisdiction in respect to a limited set of norms is consistent with principles of international comity. That is, allowing every nation's courts to adjudicate foreign conduct involving foreign parties in such cases will not significantly threaten the practical harmony that comity principles seek to protect. That consensus concerns criminal jurisdiction, but consensus as to universal criminal jurisdiction itself suggests that universal tort jurisdiction would be no more threatening. That is because the criminal courts of many nations combine civil and criminal proceedings, allowing those injured by criminal conduct to be represented, and to recover damages, in the criminal proceeding itself.[105] Thus, universal criminal jurisdiction necessarily contemplates a significant degree of civil tort recovery as well. Since different courts in different nations will not necessarily apply even similar substantive laws similarly, workable harmony, in practice, depends upon more than substantive uniformity among the laws of those nations. That is to say, substantive uniformity does not automatically mean that universal jurisdiction is appropriate. Today international law will sometimes similarly reflect not only substantive agreement as to certain universally condemned behavior but also procedural agreement that universal jurisdiction exists to prosecute a subset of that behavior.

3.3.2.1. Universal jurisdiction over criminal acts

The Princeton Principles[106] on Universal jurisdiction has the aim to clarify and bring order to an increasingly important area of international criminal law: prosecutions for serious crimes under international law in national courts based on universal jurisdiction,[107] absent traditional jurisdictional links to the victims or perpetrators of crimes. Two important and complementary means currently exist for the implementation of international criminal jurisdiction: prosecution by international criminal tribunals and the domestic application

[104] *Soda supra* note 101, at 762-3.
[105] BRIEF OF AMICUS IN *Soda supra* note 18, at *21 footnote 48.
[106] THE PRINCETON PRINCIPLES *supra* note 90.
[107] AMNESTY *supra* note 88 and research-database at <www.asser.nl>, Database of the International Committee for the Red Cross at <www.icrc.org/ihl-nat>, and *Universal Jurisdiction in Europe since 1990 for war crimes, crimes against humanity, torture and genocide* (Redress, 30 June 1999) at <www.redress.org>.

of the principle of universal jurisdiction.[108] The Princeton Principles focused on the case of "pure" universal jurisdiction, namely, where the nature of the crime is the sole basis for subject matter jurisdiction.[109]

It is jurisdiction based solely on the nature of the crime, without regard to where the crime was committed, the nationality of the alleged or convicted perpetrator, the nationality of the victim, or any other connection to the state exercising such jurisdiction.[110]

National courts can exercise universal jurisdiction to prosecute and punish, and thereby deter, heinous acts recognized as serious crimes under international law. When national courts exercise universal jurisdiction appropriately, in accordance with internationally recognized standards of due process, they act to vindicate not merely their own interests and values but the basic interests and values common to the international community.[111]

A state and its judicial organs shall observe international due process norms including but not limited to those involving the rights of the accused and victims, the fairness of the proceedings, and the independence and impartiality of the judiciary (hereinafter referred to as "international due process norms").[112]

However, improper exercises of criminal jurisdiction, including universal jurisdiction, may be used merely to harass political opponents, or for aims extraneous to criminal justice. Moreover, the imprudent or untimely exercise of universal jurisdiction could disrupt the quest for peace and national reconciliation in nations struggling to recover from violent conflict or political oppression. Prudence and good judgment are required here, as elsewhere in politics and law.

Thus, a state shall exercise universal jurisdiction in good faith and in accordance with its rights and obligations under international law.[113] This means that a person who is subject to criminal proceedings shall not be ex-

[108] Mary Robinson, U.N. High Commissioner for Human Rights' preface THE PRINCETON PRINCIPLES *supra* note 90, at 11 & 15.
[109] THE PRINCETON PRINCIPLES *supra* note 90, at 42.
[110] THE PRINCETON PRINCIPLES *supra* note 90, at 1.1.
[111] Introduction to THE PRINCETON PRINCIPLES *supra* note 90, at 23.
[112] THE PRINCETON PRINCIPLES *supra* note 90, at 1.4.
[113] THE PRINCETON PRINCIPLES *supra* note 90, at 1.5.

posed to multiple prosecutions or punishment for the same criminal conduct;[114] and a state shall recognize the validity of a proper exercise of universal jurisdiction by another state and shall recognize the final judgment.[115] Statutes of limitations or other forms of prescription shall not apply to serious crimes under inter-national law as specified in Principle 2.1.[116] A state shall, where necessary, enact national legislation to enable the exercise of universal jurisdiction and the enforcement of these Principles.[117]

"Serious Crimes under international law" includes: (1) piracy; (2) slavery; (3) war crimes;[118] (4) crimes against peace; (5) crimes against humanity; (6) genocide; and (7) torture.[119] With respect to "serious crimes under international law" as specified, national judicial organs may rely on universal jurisdiction even if their national legislation does not specifically provide for it.[120] The Treaty against transnational Organized Crimes further define "serious crimes" as conduct constituting an offence punishable by a maximum deprivation of liberty of at least four hears or a more serious penalty.[121] However the treaty does not describe what offences under public international law should be punished by four years of imprisonment;[122] and whether a plain multiplication of penalties are allowed when calculating the total time for

[114] THE PRINCETON PRINCIPLES *supra* note 90, at 9.1 – Non bis in idem.
[115] THE PRINCETON PRINCIPLES *supra* note 90, at 9.2.
[116] THE PRINCETON PRINCIPLES *supra* note 90, at 6.
[117] THE PRINCETON PRINCIPLES *supra* note 90, at 11.
[118] "War crimes" were initially restricted to "serious war crimes," namely, "grave breaches" of the 1949 Geneva Conventions and Protocol I, in order to avoid the potential for numerous prosecutions based upon less serious violations. The participants, however, did not want to give the impression that some war crimes are not serious, and thus opted not to include the word "serious." The assembly agreed, though, that it would be inappropriate to invoke universal jurisdiction for the prosecution of minor transgressions of the 1949 Geneva Conventions and Protocol I, Commentary to THE PRINCETON PRINCIPLES *supra* note 90, at 46.
[119] THE PRINCETON PRINCIPLES *supra* note 90, at 2.1.
[120] THE PRINCETON PRINCIPLES *supra* note 90, at 3.
[121] "Palermo Treaty", see above footnote 60. See also, Vienna Declaration on Crime and Justice, A/RES/55/59 at the United Nations office on Drugs and Crime <http://www.unodc.org/unodc/crime_cicp_sitemap.html> or United Nations Crime and Justice <http://www.uncjin.org> (visited November 2005).
[122] See Article 11(6).

imprisonment – as for example done in the U.S. whereas several European countries use a lump-calculation.[123]

The official position of any accused person, whether as head of state or government or as a responsible government official, shall not relieve such person of criminal responsibility nor mitigate punishment.[124]

3.3.3. ABA jurisdiction rules.

American Bar Association made in August 2000 a report "Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues created by the Internet"[125] which gives some jurisdictional default rules, amongst others the following:s

- Every Internet party should be subject to personal and prescriptive jurisdiction somewhere. In reasonable circumstances, more than one state may be able to assert both personal and prescriptive jurisdiction in electronic commerce transactions, as they have historically in physical transactions.
- Personal or prescriptive jurisdiction should not be asserted based solely on the accessibility in the state of a passive web site that does not target the state.
- Both personal and prescriptive jurisdiction should be assertable over a web site content provider in a state, assuming there is no enforceable contractual choice of law and forum, if:…(c) a dispute arises out of a transaction generated through a web site or service that does not target any specific state, but is interactive and can be fairly considered knowingly to engage in business transactions there.
- Good faith efforts to prevent access by users to a site or service through the use of disclosures, disclaimers, software and other technological blocking or screening mechanisms should insulate the

[123] "Imprisonment for life" in Denmark is maximum twenty years total, Danish Criminal Code Article 33 (2).

[124] THE PRINCETON PRINCIPLES *supra* note 90, at 5.

[125] American Bar Association, ACHIEVING LEGAL AND BUSINESS ORDER IN CYBERSPACE: A REPORT ON GLOBAL JURISDICTION ISSUES CREATED BY THE INTERNET, 55 BUSLAW 1801 (August 2000) and SPANG-HANSSEN-2 *supra* note 8, at 425-428.

sponsor from assertions of jurisdiction.

- In the interests of encouraging the growth of electronic commerce on a fair, universal and efficient basis, governmental entities should be cautious about imposing jurisdictional oversight or protections that can have extra-territorial implications in Cyberspace.
- In the interests of fairness, jurisdictional rules should be developed by and/or only after full consideration of the views of those who must abide by them and/or those substantially impacted by them.
- Self-regulatory regimes that can forge workable codes of conduct, rules and standards among a broad spectrum of electronic commerce participants may provide an efficient and cost effective jurisdictional model that governments can adopt and embrace.

The above mentioned rules covering transborder issues do not seem to be in violations to public international law on jurisdiction.

3.3.4. Global Jurisdiction

The following are examples of rules that support the particular Nation's courts to exercise "global jurisdiction",[126] unless the court interpretate the rules with limitation. However it should be emphasized, this does not necessary imply a rule is valid under public international law and thus cannot be overruled by the International Court of Justice.

3.3.4.1. Examples from Common Law

The following gives examples from common law of pure online issues related to business respectively defamatory and Global Jurisdiction.

3.3.4.1.1. United States

Restatement (Third) of Foreign Relations Law § 421 requires for allowing general[127] jurisdiction to adjudicate that defendant "regularly" carries on

[126] See above *supra* section 3.3.1.

[127] General jurisdiction is the jurisdiction not limited to claims arising out of conduct or activity in the forum state but to any case, Reporters note 3 to REST-Foreign *supra* note 12, at § 421.

business in the state, and if so the business in that state can be sued in any type of case.[128] This means for a State to have general jurisdiction to adjudicate in the Cyberspace perspective the State must - beside a requirement of reasonableness[129] - with the particular alien:

- have sufficient closeness to the forum
- the online activity must amount to what international law categorize as business
- the business must qualify to be "regularly" in the international perspective[130]
- only objective Cyberspace facts related to the State in question is counting

Use of the term "universal jurisdiction" in relation to Cyberspace has been rejected by U.S. Courts.[131]

At this place should be mentioned that many courts in the U.S. when dealing with Cyberspace issues have discussed the "sliding scale" from the Zippo case. It should be noted that the *Zippo* case only dealt with the question of specific[132] personal jurisdiction as the plaintiff in the case did not claim gen-

[128] In *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 486 (E.D.Pa. 1999) an expert divided websites into five general business models: (1) the Internet presence model, which involves no direct sales or advertising but is used by a business to raise customer awareness of the name and products of the Website operator, (2) the advertiser supported or sponsored model, in which nothing is for sale, content is provided for free, and advertising on the site is the source of all revenue, (3) the fee based or subscription model in which users are charged a fee before accessing content, (4) the efficiency or effective gains model, by which a company uses the Web to decrease operating costs, and (5) the online storefront, in which a consumer buys a product or service directly over the Web.

[129] SPANG-HANSSEN-2 *supra* note 8, at 418-424 and 430.

[130] Must be so substantial and continuous and of such nature as to justify suit against it on causes of action arising from dealings entirely distinct from those activities. Even continuous activity of some sorts within a state is not enough to support the demand to exercise general jurisdiction, *International Shoe co. v. Washington*, 326 U.S. 310, 318 (US 1945).

[131] SPANG-HANSSEN-2 *supra* note 8, at footnote 1463.

[132] Jurisdiction that stems from the defendant's having certain minimum contracts with the forum state so that the court may hear a case whose issues arise from those minimum contacts.

eral jurisdiction.[133] The *Zippo*-court speaks of a gliding scale between cases where a defendant "clearly" does business over the Internet and cases only involving a website that does little more than make information available to those who are interested in it, which the court defined a "passive website".

The following appeal courts have applied the Zippo test to general jurisdiction:[134] Fifth Circuit in *Mink* (1999)[135], Tenth Circuit in *Soma* (1999)[136], District of Columbia Circuit in *Gorman* (2002)[137], Ninth Circuit in *Gator* (2003).[138]

Other courts have found the Zippo "sliding scale less useful:[139] Fifth Circuit *Revell*[140](2002) (noting the Zippo sliding scale "is not well adapted to the general jurisdiction inquiry") and Eights Circuit *Lakin*[141] (2003)(We agree with the courts that do not apply the "sliding scale" presumptively for cases of general personal jurisdiction).

No court using the Zippo sliding scale has defined "clearly doing business" through a website as equal to the requirement allowing the exercise of general personal jurisdiction, that is substantial, continuous and systematic contacts with the forum state.

A survey[142] of US cases until January 2001 on general jurisdiction and Cyberspace shows that courts have found it extremely dangerous to claim

[133] *Zippo Mfg. Co. v. Zippo Dot Com, Inc*., 952 F.Supp. 1119, 1122 (W.D.Pa. 1997) and SPANG-HANSSEN-2 *supra* note 8, at footnote 1462.

[134] SPANG-HANSSEN-2 *supra* note 8, at footnote 1462.

[135] *Mink v. AAAA Development LLC*, 190 F.3d 333, 336 (5th Cir. 1999).

[136] *Soma Medical International v. Standard Chartered Bank*, 196 F.3d 1292, 1296-97 (10th Cir. (Utah) Dec 1999).

[137] *Gorman v. Ameritrade Corp*., 293 F.3d 506, 513 (D.C. June 2002).

[138] *Gator.com Corp. v. L.L.Bean, Inc*., 341 F.3d 1072, 1079 (9th Cir. Sep. 2003) [hereinafter *Gator 2003*].

[139] SPANG-HANSSEN-2 *supra* note 8, at footnote 1462.

[140] *Revell v. Lidov*, 317 F.3d 467, 471 (5th Cir. Dec 2002).

[141] *Lakin v. Prudential Securities, Inc*., 348 F.3d 704, 711 (8th Cir. Nov. 2003) [hereinafter *Lakin*].

[142] HENRIK SPANG-HANSSEN, CYBERSPACE JURISDICTION IN THE U.S.: THE INTERNATIONAL DIMENSION OF DUE PROCESS - 197-226 (Complex 5/01, Norwegian Research Center for Computers and Law, Oslo University 2001 - ISBN 82-7226-046-8 – US Congress Library 2003450386), free download from <www.geocities.com/hssph> [hereinafter SPANG-HANSSEN-1].

Cyberspace facts alone to allow exercise of general jurisdiction.[143] After the end of the survey, some few US appeal courts have considered general jurisdiction related to Cyberspace, but most cases has involved defendants in the U.S.[144] - not aliens.[145]

On the contrary courts have expressed facts have to be more than convincing for it to basic for general jurisdiction.[146] For example, *Molnlycke* required the websites had to be "central" to the alien's business.[147] In *Millennium*[148] "significant portions" or "repeated transmission" was not supporting general

[143] All decisions relied (also) on fact not related to computer-network facts.

[144] However, one case has come close, but lacked information on the online business' frequency and volume with the forum, *Gorman v. Ameritrade Holding Corp*., 293 F.3d 506, 510, 513 (D.C. June 2002) (Defendant in the U.S., not alien - No specific jurisdiction, but general jurisdiction might be possible when in returning the case to the lower court is was examined the frequency and volume of the firm's transactions with forums residents. On defendant's website customers could open Ameritrade brokerage accounts online; transmit funds to their accounts electronically; and use those accounts to buy and sell securities, to borrow from Ameritrade on margin, and to pay Ameritrade brokerage commissions and interest. Using e-mail and web-posting, Ameritrade transmits electronic confirmations, monthly account statements, and both financial and product information back to its customers. As a result of their electronic interactions, Ameritrade and its District of Columbia customers enter into binding contracts, the customers become the owners of valuable securities, and Ameritrade obtains valuable revenue. Pointed out that defendant's website allowed it to engage in real-time transactions with District of Columbia residents while they sit at their home or office computers "in the District of Columbia." And by permitting such transactions to take place 24 hours a day, the site makes it possible for Ameritrade to have contacts with the District of Columbia that are "continuous and systematic" to a degree that traditional foreign corporations can never even approach. Further noted that defendant's business was conducted "in the borderless environment of cyberspace" but that "Cyberspace" is not some mystical incantation capable of warding off the jurisdiction of courts built from bricks and mortar).

[145] SPANG-HANSSEN-2 *supra* note 8, at footnote 1467.

[146] A summarize over general personal jurisdiction over aliens is found in *Metro-Goldwyn-Mayer Studios v. Grokster*, 243 F.Supp.2d 1073 (C.D.Cal Jan. 2003).

[147] *Molnlycke Health Care AB v. Dumex Medical Surgical Products Ltd*, 64 F.Supp.2d 448, 452 (E.D.Pa. 1999).

[148] *Millennium Enterprises, Inc. v. Millennium Music LP*, 33 F.Supp.2d 907, 920 (D.Or.1999).

jurisdiction. *Hockerson-Halberstadt*[149] held the website activity was not so substantial and of such a nature as to justify the exercise of general jurisdiction. From December of 1998 through April of 2000, defendant had some sales in Louisiana every month with the exception of February 1999 through its website - sales in Louisiana totaled $32,252 or less than .00008 percent of the total amount of sales Costco had during that period. The court held in *Revel*[150] that the website activity was far from general jurisdiction. The website provided internet users the opportunity to subscribe to the Columbia Journalism Review, purchase advertising on the website or in the journal, and submit electronic applications for admission. Defendant had 17 subscriptions by Texas residents in 2000 and 18 for the first two issues in 2001). *Als Scan*[151] rejected general jurisdiction, even though electronic transmissions from maintenance of a website on the Internet might have resulted in numerous and repeated electronic connections with persons in Maryland. However, such transmissions do not add up to the quality of contacts necessary for a State to have jurisdiction over the person for all purposes. In *Bird* 4,666 Ohio residents registered domain names with defendant. The ability of viewers to register domain names on the website was insufficient to justify general jurisdiction, because the website simply enables defendant to do business with Ohio residents, a fact that does not permit general jurisdiction.[152] *Lakin*[153], see further below, held the percentage of a company's sales in a given state are generally irrelevant. Instead, the focus is on whether a defendant's activity in the forum state is "continuous and systematic". *Bancroft* held the contacts did not qualify as either substantial or continuous and systematic.[154]

As of November 2005 there seem only to exists one published US appeal[155] court case that have held Cyberspace facts alone allowed exercise of

[149] *Hockerson-Halberstadt, Inc. v. Propet USA, Inc*, 62 Fed.Appx 322, 2003 WL 1795641 (Fed Cir. April 2003).

[150] *Revell v. Lidov*, 317 F.3d 467 (5th Cir. Dec 2002).

[151] *Als Scan, Inc. v. Digital Service Consultants Inc*., 293 Fed 707 (4th Cir. June 2002).

[152] *Bird v. Parsons*, 289 F.3d 865 (6th Cir. May 2002). *See also, Christian Science v. Nolan*, 259 F.3d 209 (4th Cir. July 2001) (clearly no general jurisdiction).

[153] *Lakin supra* note 141, at 709.

[154] *Bancroft & Masters, Inc. v. Augusta Nat'l Inc*., 223 F.3d 1082, 1086 (9th Cir. 2000).

[155] A published lower court decision has also exercised general jurisdiction: *Directory Dividends, Inc v. SBC Communications, Inc*, 2003 WL 21961448 at * 7-8 (E.D.Pa.

general jurisdiction. This case dealt with a defendant, which was a US-resident - not an alien. Furthermore, the case was reheard en banc[156] and declared moot in February 2005[157] before the court had made a final decision on the general jurisdictional question dealt with in its September 2003 decision.

3.3.4.1.1.1 Gator.com v. L.L. Bean, Inc. – the September 2003 Decision

In *Gator.com*[158] the Court of Appeals for the 9th Circuit initially pointed out that standard for establishing general jurisdiction is "fairly high".

The issue was whether Bean's contacts with California as a result of its sales and other activities in California were "substantial, continuous and systematic," as the District Court had determined it did not have in personam jurisdiction. Ninth Circuit held defendant's substantial mail-order and internet-based commerce in the state, were sufficient to support the assertion of general personal jurisdiction and reversed.

What is interesting about the case is that the Ninth Circuit held that:[159]

"even if the only contacts L.L. Bean had with California were through its virtual store, a finding of general jurisdiction in the instant case would be consistent with the "sliding scale" test that both our own and other circuits

July 2003) (Defendant a US-resident - Could buy Cingular Wireless phones and SBC products over the Internet for use in Pennsylvania. By clicking "Pennsylvania" on a pull down menu or by entering a Pennsylvania zip code initiated on the screen a list of SBC products and services offered in Pennsylvania. Held: Defendant specifically targets Pennsylvania with its website by providing services tailored to the needs of Pennsylvania residents. This specifically intended Internet contact with Pennsylvania was sufficiently systematic and continuous that the website alone may be used as the basis for a finding of general personal jurisdiction).

[156] *Gator.com Corp. V. L.L.Bean, Inc*., 366 F.3d 789 (9th Cir. April 29, 2004). In October 2003, Gator has changes its name to Claria Corporation, Stefanie Olsen, *Gator sheds skin, renames itself*, News.com, October 29, 2003 at <http://news.com.com/2100-1024_3-50999212.html> (visited December 2003).

[157] *Gator.com Corp. V. L.L.Bean, Inc*., 398 F.3d 1125 (9th Cir. Feb. 15, 2005).

[158] *Gator 2003 supra* note 138. It reversed a decision of Nov 21, 2001 from the N.C. Cal., .

[159] As the 9th Circuit decided general jurisdiction, the court did not make a special jurisdiction analysis, see decision footnote 2.

have applied to internet-based companies.[160] This test requires both that the party in question "clearly [do] business over the Internet,"[161] and that the internet business contacts with the forum state be substantial or continuous and systematic. Recognizing that an online store can operate as the functional equivalent of a physical store, the test does not require an actual presence in the state. Rather, the nature of the commercial activity must be of a substantial enough nature that it "approximate[s] physical presence.""(citations omitted).[162]

> Bean is a Maine corporation with its principal place of business in that state. It sells clothing and outdoor equipment and maintains stores in Maine, Delaware, New Hampshire, Oregon, and Virginia. In total, L.L. Bean sells over one billion dollars worth of merchandise annually to consumers in 150 different countries. A very large percentage of L.L. Bean's sales come from mail-order and internet business. Bean also maintains relationships with numerous California vendors.
>
> Gator.com Corp. is a Delaware corporation with its principal place of business in California. It develops and distributes software to consumers who purchase goods or services over the Internet. The Gator program displays a pup-up window offering the user a coupon for a competitor to the website the user had searched in the URL-field of the browser – if a competitor has made an agreement with Gator. Thus, Gator users who visit Bean's website are offered coupons for one of Bean's competitors via a pop-up window that at least partially obscures Bean's website. On March 16, 2001, Bean's counsel mailed Gator a cease-and-desist letter requesting that Gator stop its pop-up windows from appearing when customers visited Bean's website. On March 19, 2001, Gator filed a declaratory judgment action requesting a judgment that the Gator program did not violate any federal or state law. On July 16, 2001, L.L. Bean filed a Motion to Dismiss because the court lacked personal jurisdiction.
>
> California permits the exercise of personal jurisdiction to the full extent permitted by due process.
>
> In 2000, its website sales accounted for over two hundred million, or about 16 percent, of its total sales.

[160] Cybersell at 417-419.
[161] Zippo at 1124.
[162] *Gator 2003 supra* note 138, at 1979.

> A September 2000 New York Times article described L.L. Bean as "an e-commerce star that is out-performing all but a few companies in its categories on the Web." Bob Tedeschi, L.L. Bean Beats the Current by Staying in Mid-stream, N.Y. Times, Sept. 20, 2000, at H7. The same article quoted an L.L. Bean senior executive as stating that "[t]he Web is the fastest-growing, most profitable source of revenue for [L.L. Bean],...[a]nd it's been the primary area for generating new customers."
>
> Bean is not authorized to do business in California. However, in the year 2000 alone, L.L. Bean sold millions of dollars worth of products in California (about six percent of its total sales) through its catalog, its toll-free telephone number, and its Internet website.
>
> It maintained substantial numbers of "on-line" accounts for California consumers.

The Ninth Circuit began its analysis by pointing out that "whether dealing with specific or general jurisdiction, the touchstone remains purposeful availment to ensure that a defendant will not be haled into a jurisdiction solely as a result of random, fortuitous, or attenuated contacts. The goal give the corporation clear notice that it is subject to suit in the forum State so that it "can act to alleviate the risk of burdensome litigation by procuring insurance, passing the expected costs on to customers, or, if the risks are too great, severing its connection with the State." (citations omitted)[163]

The contacts with the forum state must be of a sort that "approximate physical presence". The terms "present" or "presence" are used merely to symbolize those activities of the corporation's agent within the state which courts will deem to be sufficient to satisfy the demands of due process. Factors to be taken into consideration are whether the defendant makes sales, solicits or engages in business in the state, serves the state's markets, designates an agent for service of process, holds a license, or is incorporated there. We focus upon the "economic reality" of the defendants' activities rather than a mechanical checklist. Also, the assertion of general jurisdiction must be reasonable.[164]

[163] *Gator 2003 supra* note 138, at 1076.
[164] *Gator 2003 supra* note 138, at 1077.

The Appeal court further noticed that in applying the "substantial" or "continuous and systematic" contacts test, courts have focused primarily on two areas.

First, they look for some kind of deliberate "presence" in the forum state, including physical facilities, bank accounts, agents, registration, or incorporation.

In addition, courts have looked at whether the company has engaged in active solicitation toward and participation in the state's markets, i.e., the economic reality of the defendant's activities in the state.

Next, the court pointed out that no Supreme Court cases and only a handful of Ninth Circuit cases had addressed the issue of when and whether general jurisdiction may be asserted over a company that does business on the internet.

The court found the instant case was a close question.[165]

It held Bean's website was "highly interactive and very extensive: L.L. Bean "clearly does business over the Internet." See Zippo, 952 F.Supp. at 1124. Moreover, millions of dollars in sales, driven by an extensive, ongoing, and sophisticated sales effort involving very large numbers of direct email solicitations and millions of catalog sales, qualifies as "substantial" or "continuous and systematic" commercial activity."[166]

As for the Reasonableness Test, the court found that L.L. Bean has not presented a compelling case that general jurisdiction is unreasonable.[167]

The court noted finally, that it "It is increasingly clear that modern businesses no longer require an actual physical presence in a state in order to engage in commercial activity there. With the advent of "e-commerce," businesses may set up shop, so to speak, without ever actually setting foot in the state where they intend to sell their wares. Our conceptions of jurisdiction must be flexible enough to respond to the realities of the modern marketplace. As technological progress increases the flow of commerce between States, the need for jurisdiction over nonresidents undergoes a similar increase. In response to these changes, the requirements for personal jurisdic-

[165] *Gator 2003 supra* note 138, at 1978.
[166] *Gator 2003 supra* note 138, at 1080.
[167] *Gator 2003 supra* note 138, at 1081.

tion over nonresidents evolve. Businesses who structure their activities to take full advantage of the opportunities that virtual commerce offers can reasonably anticipate that these same activities will potentially subject them to suit in the locales that they have targeted."[168]

It should be pointed out that the 2003 decision has been recalled.

> The Ninth Circuit later allowed rehearing of the case en banc but did never finally decide on the jurisdictional issue as the court declared the case for moot because the parties after the hearing had made an agreement. The three of eleven judges that dissented noticed that the decision Gator.com Corp. v. L.L. Bean, Inc., 341 F.3d 1072 (9th Cir. 2003) "no longer has the force of law."[169]

The 2003 decision has a different view than that of the Fifth Circuit, which has stated, "given the nature of general jurisdiction, corporations have a right to structure their affair to avoid the general jurisdiction of state's courts,"[170] see next on a case with a alien defendant.

3.3.4.1.1.2 Lakin v. Prudential Securities

The Eights Circuit has disagreed with *Gator 2003* decision in *Lakin*[171] as it held the percentage of a company's sales in a given state is generally irrelevant when deciding the question of "continuous and systematic" activity. It noted defendant's local sales in Gator only accounted for six percent of its total sale and pointed out the important inquiry rather focuses on whether the

[168] *Gator 2003 supra* note 138, at 1081.

[169] *Gator.com Corp. V. L.L.Bean, Inc*., 398 F.3d 1125, 1132, 1142 (9th Cir. Feb. 15, 2005). 3 out of 11 judges dissented.

[170] *Mink v. AAAA Development LLC*, 190 F.3d 333, 337 (5th Cir. 1999)(A website containing advertising, a toll-free phone number, a printable order form, a mailing address and an e-mail address, which did not accept orders, but allowed the defendant to reply to e-mail initiated by website visitors, was insufficient to establish general personal jurisdiction), *Westcode, Inc. v. RBE Electronic, Inc*, 2000 WL 124566 at * 6 (E.D.Pa. 2000)(The existence of a click-agreement on a website that does not engage in "electronic commerce" is not enough to permit general jurisdiction).

[171] *Lakin supra* note 141, at 707. Initially the appeal court held special jurisdiction was not possible over defendant that was a U.S. resident, not an alien. See also decision in footnote 169 that made the *Gator 2003* decision no longer in force.

defendant's contacts are continuous and substantial in the forum.

Further, it is not relevant whether the percentage of a company's contact is substantial for that company; rather the inquiry focuses on whether the company's contacts are substantial for the forum. Thus, the size of the percentage of [defendant's] total business represented by its forum contacts is in general irrelevant" and "absolute amount of dollars" is not completely persuasive. More convincing is the nature of the deposits and the fact that the loans and deposits were "central to the conduct of its business.

> Defendant - with no physical existence in the forum state - maintained home-equity loans and lines of credit to Missouri residents totaling around $10 million, or one percent of its loan portfolio and a Web site on which defendant's services are offered to Missouri residents.

As for the Internet contacts, the court held that the *Zippo* "sliding scale" should not apply presumptively for cases of general jurisdiction (but was an appropriate approach in cases of specific jurisdiction) as the "nature and quality" of contacts is only one factor to consider in relation to general jurisdiction; rather a variety of factors – depending on the circumstances – has to be considered in a personal jurisdiction analysis.[172]

Three primary factors are:[173]

- The quantity of the contracts, which must be both continuous and substantial
- The nature and quality of contacts, which must be both continuous and substantial
- Further has to be considered in relation to reasonableness:
    - The interest of the forum state
    - The convenience of the parties

The court found the Zippo test has no quantity of contacts and held the Zippo test "is not well adapted to the general jurisdiction inquiry, because even repeated contacts with forum residents by a foreign defendant may not constitute the requisite substantial, continuous and systematic contacts required for a finding of general jurisdiction."

[172] *Lakin supra* note 141, at 711 and footnote 11.
[173] *Lakin supra* note 141, at 712.

The court noted defendant had a sophisticated, interactive Web site in which a user could exchange information with the host computer; exchange electronic mail; establish and access secure online accounts; calculate home-mortgage rates; and complete online applications for home-equity loans and lines of credit. The court found defendant through its website could have continuous, significant contacts with forum residents, twenty-four hours a day, thus it was possible defendant might "have contacts with the State of Missouri that [were] "continuous and systematic' to a degree that traditional foreign corporations can never even approach."

However, this was not sufficient for general jurisdiction.[174] The court had also to consider the quantity of contacts defendant had through its website with forum residents.

The plaintiff could not meet this second factor at the moment as the record did not contain indication of: the number of times that Missouri consumers had accessed the Web site; the number of Missouri consumers that had requested further information about defendant's services; the number of Missouri consumers that had utilized the online loan-application services; the number of times that a defendant representative had responded to Missouri residents after they had applied for a loan; the number and amounts of home-equity or other loans that resulted from online-application submission by Missouri consumers, or which were secured by Missouri property.[175] The court reversed the ruling on general jurisdiction and remanded this matter to the district court for jurisdictional discovery.

3.3.4.1.2. U.K. - Libel

The House of Lords in *Berezosky v. Forbes* noted about an on-line version of a magazine on the Internet and the jurisdiction that there was not the necessary evidence before the House to consider this important issue satisfactorily. Thus, the availability of the article on the Internet was, opposite the lower

[174] *Lakin supra* note 141, at 712.
[175] *Lakin supra* note 141, at 703.

court, not discussed.[176]

The High Court in *Schwarzenegger*[177] asserted jurisdiction over an Internet libel suit launched against California Governor Arnold Schwarzenegger. The suit arose from an article in the LA Times available online that discussed an alleged sexual harassment. The court held an "internet publication takes place in any jurisdiction where the relevant words are read or downloaded."

3.3.4.1.3. Canada – Libel

The Ontario Court of Appeal unanimously held Ontario courts did not have jurisdiction to hear a case involving American Washington Post and a defamatory[178] statement available in Canada through the Internet.[179]

In 1997, when Guinean-born and Guinean national Cheickh Bangoura worked for the United Nations in Kenya, the Washington Post published two articles relating to Bangoura's conduct in a previous UN posting on the Ivory Coast. The newspaper had no wholesale distribution in Canada[180] and had only seven paid subscribers in Ontario. The articles were freely available online for 14 days after publication, but thereafter only accessible through a paid archive.[181]

Six years after publication, and almost three years after moving from Africa to the Canada as an immigrant in 1997, Bangoura raised proceedings in an Ontario court against both the newspaper and three of its reporters, seeking an injunction, a retraction and $10 million in damages. He became a Canadian citizen in 2001 and had the last two years lived in Ontario where he

[176] *Berezosky v. Michaels & Berezosky v. Forbes*, [2000] E.M.L.R. 643, 657. Lower court decision *Berezovsky v. Forbes Inc*., [1999] I.L.Pr. 358, 1998 WL 1043805, [1999] E.M.L.R. 278, (English Court of Appeal, 1998).

[177] *Anna Richardson v. Arnold Schwarzenegger, Sean Walsh and Sheryl Main* [2004] EWHC 2422 (High Court, Queens Bench Division, October 29 2004 – case no. HQ04X01371). *See also*, Case Comment: *Arnold Schwarzenegger Case not Terminated*, Entertainment Law Review 2005, Ent. L.R. 2005, 16(6), 156-158.

[178] *Cheickh Bangoura v. Washington Post*, 2005 CarswellOnt 4343 paras 18 (Ontario court of Appeal, September 16 2005) [hereinafter *Bangoura 2005*].

[179] *Bangoura 2005 supra* note 178, at para 46.

[180] *Cheickh Bangoura v. Washington Post*, 2004 CarswellOnt 340 (Ontario Superior Court of Justice, 27 January 2004).

[181] *Bangoura 2005 supra* note 178, at paras 1 and 11.

now worked.[182]

The Appeal Court distinguished the circumstances from those of Joseph Gutnick[183] who raised a claim in Australia over a US publication. Gutnick was a well-known businessman who resided in Victoria at the time of the impugned publication…and there was evidence that Barron's had some 1,700 Internet subscribers in Australia. Gutnick undertook that he would sue only in Victoria and only in respect of damages to his reputation in that state.[184]

The Canadian Appeal court held that the connection between Bangoura's claim and Ontario was "minimal at best",[185] and there was no evidence that Bangoura had suffered significant damages in the province.[186] Furthermore, it was not reasonably foreseeable in January 1997 that Mr. Bangoura would end up as a resident of Ontario three years later. To hold otherwise would mean that a defendant could be sued almost anywhere in the world based upon where a plaintiff may decide to establish his or her residence long after the publication of the defamation.[187] Furthermore was noted, that there was no evidence that the Washington Post had insurance coverage in Ontario.[188]

The court pointed out, that where the case is international in nature, rather than interprovincial, it is more difficult to justify the assumption of jurisdiction.[189] In addition, it remarked that the Washington Post defendant's home jurisdiction's unwillingness to enforce such an order is not determinative of whether the court should assume jurisdiction.[190] On February 16, 2006, the

[182] 2004 CarswellOnt 340 para 7-8.

[183] *Dow Jones v. Gutnick*,[2002] HCA 56 paras 28, 42 & 44, 42 I.L.M. 41, 2002 WL 31743880, 210 CLR 575, 194 ALR 433, 77 ALJR 255, [2003] AIPC 91-842 (High Court of Australia, 10 December 2002 - No. M3/2002) <http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html> (visited 10 December 2002). In a out-of-court settlement of November 2004, Gutnick was awarded $180,000 and in cost $400,000, *Gutnick 'delight' on defamation deal*, THE AUSTRALIAN, November 12, 2004 at <http://www.theaustralian.news.com.au/common/story_page/0,5744,11365187%255E1702,00.html> (visited November 15, 2004).

[184] *Bangoura 2005 supra* note 178, at paras 43-44.

[185] *Bangoura 2005 supra* note 178, at para 22.

[186] *Bangoura 2005 supra* note 178, at para 23.

[187] *Bangoura 2005 supra* note 178, at para 25.

[188] *Bangoura 2005 supra* note 178, at para 27.

[189] *Bangoura 2005 supra* note 178, at para 35.

[190] 2004 CarswellOnt 340 para 23.

Supreme Court of Canada refused leave to appeal.[191]

3.3.4.2. Example from Civil Law

The following is an example from a civil law country of a statute that from its wording allows Global jurisdiction[192] in pure online issues – unless the courts interpretate the statute in a very narrow way.

3.3.4.2.1. Denmark

Article 246 of the Civil Procedure Code[193] determines whether courts in Denmark has jurisdiction over an alien,[194] which is not a citizen of another Member State of the E.U. or the Nordic countries. It states:

> Subsection 1. Lawsuits against persons, corporations, associations, private institutions and other kinds of organization that does not have "home jurisdiction" in Denmark can be brought in Denmark if any court pursuant to §§ 237, 238, subsections 2, 241, 242, 243 and 245 can be regarded as jurisdiction for the case. [See Appendix 7]. In lawsuits concerning consumer contracts, the consumer can bring a lawsuit against the said persons and organizations at the consumers "home jurisdiction" if a special offer or advertising in Denmark

[191] *Cheickh Bangoura v. Washington Post*, 2006 CarswellOnt 932 (Supreme Court of Canada, February 16, 2006 – Docket 21203).

[192] On other examples, see AKEHURST *supra* note 19, at 156, 172, 199 & 234.

[193] [U.K.:] Administration of Justice Act. The latest consolidated version of the Danish Procedure Code is printed as No. 910 of 27/09/2005 with amendment from Laws No. No. 525 of 24/06/2005, 542 of 24/06/2005, 552 of 24/06/2005, 554 of 24/06/2005, 1398 of 21/12/2005 and 1399 of 21/12/2005. Unofficial translation into English by Henrik Spang-Hanssen of §246 of Retsplejeloven in Appendix 7.

[194] A person is procedural foreigner if he by residence or stay has a stronger link to foreign countries than Denmark. Citizenship is without any importance. "Foreigner" are: (1) a person living abroad without residence in Denmark, (2) a person that stay in foreign countries without link to the Danish territory or without previous residence in Denmark, and (3) a person that stay in Denmark with residence outside Denmark. See BETÆNKNING NR. 1052 AF 1985 OM RETTERNES STEDLIGE KOMPETENCE I BORGERLIGE SAGER [Report no. 1052 of year 1985 on the jurisdiction of courts in civil cases] 18 and chapter 4, KARNOV LOVSAMLING [Karnov statute book] Vol. 3 note 999 (17. Ed., 2001) and Folketings Tidende [Official Journal of Danish Parliament] 1985-86, Supplement A, column 2940.

> was made before the agreement was entered into and the necessary actions for the fulfillment of the agreement were made by the consumer in Denmark.
>
> Subsection 2. If no court can be regarded as having jurisdiction in the case pursuant to subsection 1, then lawsuits concerning financial circumstances against the persons mentioned in subsection 1 can be brought at the court at the place, where the [natural] person stayed at the time of service of process.
>
> Subsection 3. If there is no jurisdiction according to subsection 1, lawsuits concerning financial circumstances against the persons and organizations mentioned in subsection 1 can be brought at court at the place where the defendant has property at the time of filing the suit or where the property that the dispute concerns is located at the time when the suit is filed. If arrest of property (as an interim remedy) is avoided by giving security, the security is regarded as property located where the application for attachment was or should have been filed.

When determining the international competence of Danish courts, Denmark is regarded as one jurisdiction, and one speaks of the courts international competence or jurisdiction-rules.

It should also be pointed out that the Danish jurisdiction-rules does not allow courts in Denmark to reject cases, even though the judge feels it is unfair to adjudicate a certain case caused by the international aspects of the case - here, transborder transmission of electronic bits on international computer networks. In Denmark a court does not have any discretion to reject a case as long as it is in accordance with the rules of international jurisdiction. The doctrine of forum non-convenience is not used in Denmark.

Thus, the courts in Denmark have competence in all cases with international aspects.

Pursuant to international procedural rules Danish courts lacks competence if a sufficient links to Denmark does not exist. The points of contact in public international law[195] is not necessarily the same as in (Danish) private international law; and the requirements in public international law is different for legislative (prescribe and adjudicate) and enforcement jurisdiction.

The Danish jurisdiction-rules do not require the case has any special connection to Denmark as several of the jurisdiction-rules are based on other

[195] SPANG-HANSSEN-2 *supra* note 8, Chapters 27 and 32.

factors. Public international law - not each State's private international law – demand (beyond the requirement of a close link) predictability and fundamental fairness. This cannot be said to be obtained by all the rules of the Danish Civil Procedure Code when the issue is transborder dealings on international computer networks - outside the areas where use of §246 of the Danish Civil Procedure Code is especially prohibited, that is, the areas covering the E.U. and Lugano conventions on jurisdiction.[196]

3.4. Discussion

The following begins with the analyze initially mentioned above in section 3.3.1. This analyze does not start from the hierarchical bottom, that is, the single state's or sovereign's eye, but from the top, that is, the international society's eye. This latter has in the last decade demanded more and more that a common view of the individuals in the world shall be the primary goal rather than the individuals of a certain sovereign or state – beginning with the U.N. Charter declaration on human rights.

Thus, this analyze begins with the point of view of public international law rather than a single state's law (including private international law or Conflicts of law[197]), because another basis for the analyze on "pure online"

[196] Danish Act no. 325 of 4 June 1986 on the Brussels Convention, Article 3 of the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters, preamble no. 2 (Consolidated version of 26 January 1998 in O.J. 1998 C 027, 26/01/1998 p. 0001-0027) & Article 3 of the E.U. Council Regulation 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcements in civil and commercial matters, O.J L 012, 16/01/2001 p. 0001–0023, and Article 3 of the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters of 16 September 1988, 88/592/EEC, O.J. L 319 , 25/11/1988 p. 0009–0048. See ECJ's website <http://www.curia.eu.int> (visited May 2006). It "falls entirely within the sphere of exclusive competence of the European Community" to make a new Lugano Convention (ECJ Opinion 1/03 of 7 February 2006 - European Court reports 2006 page 00000) at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62003V0001:EN:HTML>.

[197] See for example WORLD INTELLECTUAL PROPERTY ORGANIZATION, INTELLECTUAL PROPERTY ON THE INTERNET: A SURVEY OF ISSUES 113-131, (December 2002 – Doc. WIPO/Int/02) at <http://ecommerce.wipo.int/survey/pdf/survey.pdf> (visited 2003).

incidents would imply a chaotic result with a mixture – and sometimes even opposing – views of single states on which court should rule over a cybernaut's act on the Internet.[198]

Under public international law it is a requirement – except for universal jurisdiction - for a State to deal with a transborder activity that the alien behind this has a certain link or closeness with the forum State and that it is reasonable for the forum to deal with the matter.[199]

3.4.1. Sufficient Closeness

When determining the closeness requirement in international law it is not a question of finding the closest related court, but rather to eliminate that not every court in every State in the world is allowed to deal with a certain dispute (which would be the same as "global jurisdiction"), so a alien can have some predictability of which State court's can be the possibilities - except when looking upon universal jurisdiction. Akehurst holds one should find where the "primary" effects are.[200] On the other hand, international law requires that also in case of concurrent jurisdiction the States in question have to be foreseeable. As for Cyberspace the essential and vital difference is whether the uploaded content is only reaching (can be accesses from) a State or the content is purposefully targeting that State. International law only allows objective facts and evidence to show the actual alternative - not a courts subjective determination.[201]

3.4.1.1. Universal Jurisdiction

When a court exercise universal jurisdiction it acts on behalf on the international society pursuant to public international law. Thus, the question is not whether a State can exercise universal jurisdiction but when it can do it, that is, what kind of acts of an alien allows under public international law for universal jurisdiction.

[198] *Id* at 135 no. 328.
[199] SPANG-HANSSEN-2 *supra* note 8, at 240-242.
[200] AKEHURST *supra* note 19, at 158-159, 169.
[201] SPANG-HANSSEN-2 *supra* note 8, at 382-383.

Until now, public international law has only allowed exercise of universal jurisdiction if the act were gruesome or fatal, for example piracy and slave trade, war crimes, because such crimes either are found to be devastating and ruining trade or being inhuman.

It is now widely accepted that states may exercise universal jurisdiction over piracy as a crime under international law.[202] The customary international law rule of universal jurisdiction on the high seas over piracy is now codified in the provisions of the 1982 Convention on the Law of the Sea[203] and its predecessor, the 1958 High Seas Convention.[204] The latter's article 105 states: "On the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board. The courts of the State which carried out the seizure may decide upon the penalties to be imposed, and may also determine the action to be taken with regard to the ships, aircraft or property, subject to the rights of third parties acting in good faith."

For centuries there was no generally accepted definition of the crime of "piracy" under international law.[205] A definition that reflects[206] the customary international law of piracy is given in the High Seas Convention of 1958, which was repeated in Article 101 of the 1982 Convention on the Law of the Sea that has 135 parties. Article 15 of the High Seas Convention of 1958 states: Piracy consists of any of the following acts: (1) Any illegal acts of

[202] "[I]n the case of what is known as piracy by the law of nations, there has been conceded a universal jurisdiction, under which the person charged with the offence may be tried and punished by any nation into whose jurisdiction he may come," *S.S. Lotus* (France v. Turkey) 1927 P.C.I.J. (Ser. A) No. 10 para 70 (Moore, J., dissenting), also at <www.geocities.com/hssph/Lotus.doc>; AKEHURST *supra* note 19, at 160-166; BROWNLIE, *supra* note 13, at 235; OPPENHEIM *supra* note 39, at 469; Kenneth C. Randall, *Universal Jurisdiction under International Law,* 66 TEX. L. REV. 785 (1988); SHAW *supra* note 13, at 470; REST-Foreign *supra* note 12, at § 404.

[203] Convention on the Law of the Sea of 1982 (Montego Bay Convention), U.N. Doc. A/CONF. 62/122.

[204] Convention on the High Seas of 1958, 13 U.S.T. 2312, T.I.A.S. 5200, 450 U.N.T.S. 82, Art. 15. As of May 2006, 62 states are parties to the Convention.

[205] AMNESTY *supra* note 88, at Chapter Two page 3-8.

[206] BROWNLIE *supra* note 13, at 236.

violence, detention or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (a) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (b) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State; (2) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft; (3) Any act of inciting or of intentionally facilitating an act described in sub-paragraph 1 or sub-paragraph 2 of this article.

Related to Cyberspace (public international computer network) piracy is not a common term. Neither the Cybercrime Convention[207] nor its Protocol[208] uses the term "piracy".

As for Cyberspace, deliberate, abusive and in bad-faith registration of a large number of domain names[209] ("cybersquatting" to a large extent) is regarded as extremely negatively by all cybernauts, except the offenders. However, the abusive act can only be done by the cooperation of a (neutral) registrar that seems to prevent the violation to be classified as gruesome or fatal, which is required for universal condemnation by the international society – and thus allowing universal jurisdiction. Neither can a violation by a "copycats"[210] support universal jurisdiction as the dispute also here will involve a

[207] Convention on Cybercrime of 23 November 2001 (Council of Europe - ETS No. 185) - Into force July 1, 2004 - at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> or <www.coe.int/T/E/communication_and_Research/Press/Themes_Files/Cybercrime>, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG > and Explanatory Report at <http://conventions.coe.int/Treaty/EN/projets/ FinalCyber-Rapex.htm> ((visited December 2005).

[208] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems of 28 January 2003 (Council of Europe – ETS No. 189) and Explanatory Report of December 2, 2005 at <http://conventions.coe.int/Treaty/en/Reports/Html/189.htm> (visited December 2005).

[209] SPANG-HANSSEN-1 *supra* note 142, at 106. See also below chapter 7 section 7.6.1 footnote 136.

[210] Copycats - unlike cybersquatters - register a domain name and use the address to operate a website that intentionally misleads users into believing they are doing business with someone else. Copycats either beat the legitimate organization to a domain name

(neutral) registrar as a third-party to offend the other party, whose remedy only should be to sue the offender at his home forum or at the registrar's forum.

Copyright infringement will hardly ever be an act that is pointed against the international society as a whole, but will probably always be between two persons or two relatively small groups of people. This prevents use of universal jurisdiction.

As for spam,[211] which can be quite annoying and in worst case can bring down one of several servers, should be noted that the drafters of the Cybercrime convention held such conduct should only be criminalized (as "system interference", Article 5) where the communication is intentionally and seriously hindered. However for allowing universal jurisdiction, the international society requires the violation is gruesome or fatal, which is not ordinary the case for spamming. If a spamming should brake down the whole public international computer network, there could be a reason for allowing universal jurisdiction as the situation would so extraordinary and extreme that it could be no surprise for the offender that "the whole world would come after him."

If a person in the online Cyberspace environment is notified that he or she indirectly participate in slave trade or enslavement[212] and do nothing – for

or register a close variation of an organization's domain name, *Flesher v. University of Evansville* (Supreme Court of Indiana, No. 82S04-0008-CV-477, October 2001) at <http://www.state.in.us/judiciary/opinions/archive/10010101.rts.html> (October 8, 2001).

[211] The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency, no. 69 in Explanatory Report to the convention at <http://conventions.coe.int/Treaty/EN/projets/ FinalCyberRapex.htm> ((visited December 2005). One of the co-authors to the predecessor to the e-mail Simple Transfer Protocol (SMTP), which protocols were made on the assumption and trust that no one would send "disturbing" content through the protocols, has suggested a whole new protocol with tighter authentication to work besides SMTP, Suzanne Sluizer to Paul Feste, *End of the road for STMP?*, CNET NEWS.COM, 1 August 2003 at <http://news.com.com/End+of+the+road+for+SMTP/2100-1038_3_5058610.html> (visited March 2005).

[212] Enslavement means the exercise of any or all of the powers attaching to the right of ownership over a person and includes the exercise of such power in the course of trafficking in persons, in particular women and children, Article 7 1.c. of Rome Statute of

example hosts of a website that engage in slave trade – exercise of universal jurisdiction is allowed by public international law as both the slave trade and slavery is seen as particularly atrocious crimes attracting international condemnation.[213] The same can be said about child-pornography that is worldwide condemned, if the person in the online Cyberspace environment has been notified that he or she indirectly participate and do nothing.[214] It is doubtful if universal jurisdiction can be exercises in the case of "child pornography" made totally digitalized and thus not involving any living child, as the act then cannot be classified a gruesome or fatal to a particular person, which seem to be the overall decisive for the international society to allow universal jurisdiction – even though child pornography as concept is disliked worldwide.[215]

As for offences involving other parties computers - such as interception,[216] data interference,[217] system interference,[218] computer-related forgery[219] and

the International Criminal Court of July 17, 1998 (into force 1 July 2002 - As of May 2005: 139 signatories and 100 parties), 2187 U.N.T.S. 3 (English text with corrections 1998-2002 at 90), also at <http://www.un.org/law/icc/> (visited May 2005)[hereinafter ICC Statute]. See also, Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others, 21 Mar. 1950, art. 11, 96 U.N.T.S. 271.

[213] AMNESTY *supra* note 88, at Chapter Two page 9-12. The two conventions on the High Sea does not expressly state at right under the treaties to arrest persons suspected of engaging in the slave trade on the ships visited. Article 99 (Prohibition of the transport of slaves) of the 1982 Montego Bay Convention and Article 13 of the 1958 High Seas Convention simply requires each state party to "adopt effective measures to prevent and punish the transport of slaves in ships authorized to fly its flag, and to prevent the unlawful use of its flag for that purpose" and states that "[a]ny slave taking refuge on board any ship, whatever its flag, shall ipso facto be free," AMNESTY *supra* note 88, at Chapter Three page 1.

[214] Compare Convention on the Rights of the Child of 20 November 1989 – into force 2 September 1990, U.N. Doc. A/RES/44/49 (1990).

[215] Compare definition in Article 9 of the Convention on Cybercrime of 23 November 2001 and No. 101 in the Explanatory Report to the Convention.

[216] Defined in Article 2 of the Cybercrime Convention as: the access to the whole or any part of a computer system without right.

[217] Defined in Article 3 of the Cybercrime Convention as: the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

computer-related fraud[220] – universal jurisdiction should only be allowed by the international society when the offence is interfering with huge part of the public international computer network as the requirement in public international law is the offence is involving a large amount of people around the world, not only a group or a region. Thus, interference with one or few computers or servers or a small group of computer networks, should not allow use of universal jurisdiction – except for attack on vital computers or servers on the public international computer networks, for example the DNS root-servers, in which case the offender should have sufficient awareness of the worldwide crime and risk universal jurisdiction.[221]

Misuse of devices as defined in Article 6 of the Cybercrime Convention cannot allow universal jurisdiction since this term relates to a (single) device or a computer password or access code,[222] but is not relating to the whole public international computer network or society, which is a requirement for allowing universal jurisdiction.

Some of the above mentioned acts related to Cyberspace can also be used

[218] Defined in Article 4 of the Cybercrime Convention as: the damaging, deletion, deterioration, alteration or suppression of computer data without right.

[219] Defined in Article 7 of the Cybercrime Convention as: the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

[220] Defined in Article 8 of the Cybercrime Convention as: fraud the causing of a loss of property to another person by (a) any input, alteration, deletion or suppression of computer data; (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

[221] These are the one that makes the domain name system work, see <www.root-servers.org>.

[222] the production, sale, procurement for use, import, distribution or otherwise making available of: (a) (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,; or the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5.

in what is called Information Warfare, where means such as spreading virus, hacker and Denial of Service attacks often are mentioned.

Thus it can be relevant to point out that there is little doubt that any state may exercise universal jurisdiction over most war crimes, whether committed during international or non-international armed conflict. The Additional Protocol I to the Geneva Conventions[223] gives universal jurisdiction over a particularly serious class of war crimes in international armed conflict - grave[224] breaches of those treaties.[225] Grave breaches include acts if committed in connection with an international armed conflict against persons or property protected by the relevant Geneva Convention: extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly. In addition to grave breaches, there are a wide range of prohibitions under customary and conventional international humanitarian law applicable to international armed conflict, which are considered to be war crimes and, therefore, subject to universal jurisdiction.[226]

To the extent acts in Cyberspace can be regarded as covered by the Geneva Conventions or by analogy universal jurisdiction is allowed.

On the other hand the strict interpretation and limitation of what is "grave breaches" in these international instruments imply, that it has to be extremely

[223] As of 15 April 2006, 164 parties to protocol I and 159 parties to Protocol II, from website "International Humanitarian Law – Treaties & Documents" of International Committee of the Red Cross at <www.cicr.org/ihl.nsf/Convpres?openView> (visited April 2006).

[224] See also definition in article 8(2.a) of the ICC Statute *supra* note 212. The drafters of the Princeton Principles holds that it would be inappropriate to invoke universal jurisdiction for the prosecution of minor transgressions of the 1949 Geneva Conventions and Protocol I, THE PRINCETON PRINCIPLES *supra* note 90, at 46.

[225] All but two of the 192 UN Members (Marshall Islands and Nauru) are parties to the Geneva Conventions of 1949 as of 15 April 2006, including both UN Observer states, the Holy See and Switzerland; see above footnote 222 on source.

[226] AMNESTY *supra* note 88, at Introduction page 6-7. As of 1 September 2001, approximately 120 states are known to have legislation which would permit them to exercise universal jurisdiction over certain conduct which could amount to war crimes if committed in international armed conflict or, in some cases, non-international armed conflict. Since the end of World War II Australia, Austria, Belgium, Canada, Denmark, France, Germany, Israel, Switzerland, the United Kingdom and the United States have exercised universal jurisdiction over war crimes.

serious crimes that are done "pure online" before universal jurisdiction is allowed.

It is also worth noting that many countries' military now hires computer technicians as most militaries expect future wars to involve attacks on computer and networks to diminish the enemy's vital computer systems. However, such attacks will often have great interference with the enemy's civil population that is protected to a certain degree by the Geneva Conventions. For conduct, which involves attacks on civilians or civilian objects and satisfies the popular concept of "terrorism," the UN General Assembly has adopted a number of conventions providing for universal jurisdiction.[227] Thus, head of states or governments[228] can become war criminals if they decide to attach foreign computer networks.

3.4.1.2. National jurisdiction

Under the made premise of "pure online" , "National jurisdiction" can be a problem since it is jurisdiction over aliens only decided by a single State, not the whole or overwhelming international society. The problem is that the

[227] Attacks could be made on computers or threatening information could be given online that could involve violation of (and thereby allow universal jurisdiction): International Convention for the Suppression of Terrorist Bombings of 15 December 1997 (Online manuals for making bombs) (Into force 23 May 2001. As of April 2006, 146 parties), 37 I.L.M. 249 (1998), International Convention for the Suppression of the Financing of Terrorism of 9 December 1999 (Money transfer) (Into force 10 April 2002. As of April 2006, 152 parties), 39 I.L.M. 270 (2000), Convention against Transnational Organized Crime of 15 November 2000 (Into force 29 September 2003. As of April 2006, 119 parties), A/RES/55/25 (G.A.O.R., 55th Sess., Supp. No. 49), Convention against the Recruitment, Use, Financing and Training of Mercenaries of 4 December 1989 (Into force 20 October 2001. As of April 2006, 28 parties), 29 I.L.M. 89 (1990), Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 23 September 1971, 974 U.N.T.S. 177, Hague Convention for the Suppression of Unlawful Seizure of Aircraft of 16 December 1970, 860 U.N.T.S. 105 (Hijacking), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation of 10 March 1988 (Navigation at sea), 1678 U.N.T.S. 222, AMNESTY *supra* note 88, at Chapter Thirteen pages 4, 5, 6, 9, 13, 15-18, 21.

[228] The official position of any accused person, whether as head of state or government or as a responsible government official, shall not relieve such person of criminal responsibility nor mitigate punishment, THE PRINCETON PRINCIPLES *supra* note 90, at 5.

receiver (plaintiff) has unlimited access to information on the Internet, where it is not a condition under the present Internet-protocol that the other party (the uploader of information) always require special access-code to get the information. Quite the opposite, the Internet functions with the premise that most possible number of people can access to largest possible information. This was also the primary aim for making the HTTP-protocol in 1991, which latter made the number of network-users explode to 800 million in 2005.[229] Thus, the Internet with its main protocols with their geography-free nature is far from build to allow a "community standards" test, which "would essentially require every Web communication to abide by the most restrictive community's standards."[230] Furthermore, "democracy doesn't work if you can turn off anyone you don't want to hear from."[231]

It is the computer technology that has created the new situation, not legal rules, that was made before the invention of international computer networks, which allow worldwide access to information and business possible and is build to disregard any national borders and prevent any hindering. When dealing with the sea or air it is a fact that a ship or airplane cannot be everywhere at the same time. Otherwise with Internet websites that can be looked upon from many places at the same time. This possibility makes it - opposite in the maritime law and aviation law - difficult to determine where the "actual (legal) location" is.[232]

Reading the wording of §246 of the Danish Civil Procedure Code on jurisdiction over aliens shows how this statute makes essential universal over all the worlds cybernauts. This is not accepted by the international society. Luckily for alien cybernauts, the Danish courts so far have interpretated the reach of statute to be very limited.

[229] See Appendix A "Estimated evolution on Online Linguistic Population" in SPANG-HANSSEN-2 *supra* note 8, at 534.

[230] *Reno v. American Civil Liberties Union*, 521 U.S. 844, 877 (US, 1977).

[231] Lessig in SACRAMENTO BEE, December 5, 1997.

[232] Henrik Spang-Hanssen, *Filtering and blocking of websites content and legislation on the Internet - including the Yahoo case* at <www.geocities.com/hssph> under Articles (Translation of article *Filterblokerng af websiders indhold og lovgivning af Internettet – herunder Yahoo*-sagen on page 321-328 in Kritisk Juss [Norwegian Law Journal "Critical Law"] No. 3-4/2001, Norway, ISSN 0804-7375).

It is necessary to give time for and the issue thoroughly consideration. It is far from today to say, that sufficient research and knowledge on the legal aspects and the technology has been achieved. U.S. Justice Souter remarked in a case, that "we should be shy about saying the final word today about what will be accepted as reasonable tomorrow. In my own ignorance I have to accept the real possibility that if we had to decide today just what the First Amendment should mean in cyberspace we would get it fundamentally wrong."[233]

In this respect it is essential to note that jurists who will legislate the Internet has to have technical knowledge, because otherwise the jurist, who has no technical education, gets special difficulties when going to deal with the edp-related facts, in a similar way he would require of himself in other areas of law.[234]

It is also very important that there must be continuity in the field on which legislation is made. As for law dealing with the Internet, that is a technical media, this is a problem as the lifespan of software and other computer technology is only six to ninth month, which is shorter than the time it takes to formulate a bill and much shorter than the time it takes to arrange international conferences for making treaties.[235]

Some scholars talk about the spillover effect of websites and has made reference to antipollution. They argue, that a cybernaut or cyberspace content provider cannot necessarily claim ignorance about the geographical flow of information as a defense to the application of the law of the place where the information appears.[236] However, while air-pollution generally is not accepted by the international society, free speech and exchange of point of views are more than acceptable in the international society - rather it is preferable, confer the U.N. Declaration on Human Rights on speech.

[233] *Denver Area Educational Telecommunications Consortium, Inc. v FCC*, 518 U.S. 727, 777 (U.S. 1996).

[234] Danish Law Professor Mads Bryde Andersen, *Förändres juristens arbetsmetoder? i Edb, lovgivningen og juristenes rolle*: Nordisk årbok i rettsinformatikk 1990 page 116-117.

[235] See *supra* note 232.

[236] See for example Jack L. Goldsmith, *Against Cyberanarchy*, UNIVERSITY OF CHICAGO LAW REVIEW, 65 U. Chi. L. Rev. 1199, 1244 (1988).

It is therefore the task in the following to look at different kind of National Jurisdiction rules and check whether these disturb the world outside the particular forum state.

3.4.1.2.1. Restricted Jurisdiction

To the extent that a national jurisdiction rule is under the term of "Restricted jurisdictions" that limits the states jurisdictional reach, see above section 3.3.1 in fine, the jurisdictional rule related to "pure online" cases will not violate public international law, as the rule does not interfere with the act's of aliens.

3.4.1.2.2. Global Jurisdiction

Rules that allow "Global jurisdiction" involve rules that gives jurisdiction over aliens being anywhere in the world. Such rules can be in violation with public international law if there is not a sufficient closeness, see above section 3.4.1.

As for global jurisdiction, limits has to be made by public international law, as it is not under public international law – opposite universal jurisdiction – accepted for every state to have jurisdiction over an alien cybernaut in any instance of "pure online." This is because under public international law it is not acceptable that worldwide access to the information imply jurisdiction over every cybernaut in the world.

Thus, limits must be drawn by public international law in relation to "pure online" cases as public international law is supreme and thereby restricts the law (jurisdictional rules) of the states in the world. F.A. Mann argues that a State may not apply its law unless there is a close connection between the State and the person, thing or event to which the law is to be applied.[237]

In the analyze of global jurisdiction it does not matter whether the national jurisdictional rule is classified as a general, specific or limited rule. The inquiry is on whether the rule has global reach or is limited to "Restricted jurisdiction," which latter creates no problems under public international law.

If a jurisdictional rule is global, then public international law has to make

[237] MANN-1 *supra* note 55, at 36-62.

some demarcation in relation to pure online cases as it otherwise would be the same as allowing universal jurisdiction. A national rule that allows jurisdiction over an alien defendant just because its information can be accessed by any forum is not having the necessary sufficient closeness to permit the rule and does neither fulfill the reasonableness requirement of public international law.

U.N. Secretary General Kofi Annan has stated, that the communication revolution has "redefined" the traditional notion of state sovereignty. We need to adapt our international system better to a world with new actors, new responsibilities, and new possibilities for peace and progress. State sovereignty, in its most basic sense, is being redefined - not least by the forces of globalization and international co-operation. States are now widely understood to be instruments at the service of their peoples, and not vice versa. At the same time individual sovereignty - by which I mean the fundamental freedom of each individual, enshrined in the charter of the UN and subsequent international treaties - has been enhanced by a renewed and spreading consciousness of individual rights.[238]

Louis Henkin - the reporter of the Restatement of Foreign Relation Law - has even stated that sovereignty is a mistake, a mistake built upon mistakes, which has barnacled an unfortunate mythology. Sovereignty has been transmuted into an axiom of the inter-state system, which has become a barrier to international governance, to the growth of international law, and to the realization of human values. He suggests the need to deconstruct the concept, strip it of its myth, identify its essentials, and retain only its valuable values.[239] Others agree that the era of sovereignty as a universal organizing principle for the management of the global system has ended.[240]

The ease with which information can now be moved across national boundaries has seriously and directly challenged the claim of the nation-state.

[238] U.N. Secretary General Kofi Annan, *Two Concepts of Sovereignty*, THE ECONOMIST at 49, 18 September 1999, at <http://www.un.org/News/ossg/sg/stories/kaecon.html> (visited November 25, 2005).

[239] Louis Henkin, *Human Rights and State "Sovereignty"*, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 25 GA. J. INT'L & COMP. L. 31-32 (1995/96).

[240] Christopher Clapham, *Sovereignty and the Third World State*, Political Studies, 47 Pol.Stud. 522, 537 (1999) XLVII.

Information can be gathered by satellites on or about other countries or citizens without the knowledge or consent of the target countries (remote sensing – RMS). Philip Allott has observed that our independence is a function of what we control and what we do not control.[241] Also, should be remembered that the business-world gets more and more transnational whereby transborder data flow (TBDF) is happening between a parent company and its subsidiaries in different countries with total disregard of national borders.

No one mode of communication illustrates more clearly than Cyberspace how the conventional notion of territorial sovereignty is being challenged by the communication revolution.[242] National borders have just become speed-bumps on the information superhighway.

Under public international law it is a requirement that people have notice of what legislation they are bound by. Physical boundaries generally have signposts that provide warning that we will be required, after crossing, to abide by different rules. Cyberspace, on the other hand, lacks such signposts informing individuals of the obligations assumed by entering into a new, legally significant, place. Individuals are unaware of the existence of those borders as they move through virtual space.[243]

As for freedom of expression, to discover the limits public international law places on nations attempting to restrict freedom of expression, one can look to the terms of the International Covenant on Civil and Political Rights (hereinafter ICCPR)[244] and how they have been interpreted by the ICCPR's adjudicatory branch, the Human Rights Committee.[245] The ICCPR basically

[241] PHILIP ALLOTT, THE HEALTH OF NATIONS: SOCIETY AND THE LAW BEYOND STATES 404 (2002 - ISBN 0521016800).

[242] Adeno Addis, *The Thin State in Thick Globalism: Sovereignty in the Information Age*, 37 Vand. J. Transnat'l L. 1, 42 (2004).

[243] David R. Johnson & David Post, *Surveying Law and Borders – The Rise of Law in Cyberspace*, 48 Stan.L.Rev 1367, 1370, 1375 (1996).

[244] 999 U.N.T.S. 171.

[245] U.N. Human Rights Committee, at <http:// www.unhchr.ch/html/menu2/6/hrc.htm> (visited October 2002). See for example, *Leo R. Hertzberg et. al. v. Finland,* Communication No. R.14/61, U.N. Doc. Supp. No. 40 (A/37/40) at 161 (1982), Communication No. 61/1979 (Fifteenth session), CCPR/C/15/D/61/1979 (Jurisprudence) at 124, 126 (Views of the Human Rights Committee under article 5, paragraph 4, of the Optional Protocol to the International Covenant on Civil and Political Rights. The court

codifies the provisions in the Universal Declaration of Human Rights (UDHR) protecting the rights of individuals to freely express their opinion and is a universally recognized document, signed by more than 122 nations from all continents. At least some provisions of the ICCPR reflect norms of customary international law and are therefore also binding on non-party nations.[246]

ICCPR article 19 states:

- Everyone shall have the right to hold opinions without interference.
- Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
- The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
    - For respect of the rights or reputations of others
    - For the protection of national security or of public order, or of public health or morals.

ICCPR article 20 states:

- any propaganda for war shall be prohibited by law, and
- any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

The nature of the challenge from the Internet is further reaching than the impact of communication technologies that preceded it. The Internet demon-

established a "margin of discretion" standard) at <http://www1.umn.edu/humanrts/undocs/session37/14-61.htm> (visited November 25, 2005).

[246] Walter C. Dauterman, *Internet Regulation: Foreign actors and local harms - At the crossroads of pornography, hate speech, and freedom of expressio*n, 28 N.C. J. INT'L L. & COM. REG. 177, 212-3 (2002).

strates the deconstitutive and constitutive dimensions of the communication revolution, and this revolution has seriously destabilized the traditional view of territorial sovereignty.[247]

Determining whether particular Internet activities satisfy requirement of sufficient closeness or minimum contacts calls for sensitivity to the fact that some Internet activities may have no meaningful analogues to traditional forms of communication, and that these activities therefore must be assessed differently. The search for a uniform test encompassing the whole of Internet jurisdiction issues is ultimately a misguided exercise, and one that has caused much of the disarray in Internet jurisdiction jurisprudence.[248]

3.4.1.2.2.1. Transnational Jurisdiction

As for "Transnational jurisdiction" as defined in the Treaty against Transnational Organized Crimes there is no violation of public international law on jurisdiction as far as the act is committed in or substantial committed in the forum state.

However, the problem with the definition is that it also allow jurisdiction where the act is committed in one state but has substantial effects in another state.[249] This problem is similar with the problems that arise under "Specific and General Jurisdiction" and thus the closeness requirement in public international law between the forum and the alien, see next.

3.4.1.2.2.2. Specific and General Jurisdiction

From the eye of the international society or public international law there is no difference between whether a jurisdiction rule is categorized specific or general. For public international law the essential is whether the rule fulfills

[247] Adeno Addis, *The Thin State in Thick Globalism: Sovereignty in the Information Age*, 37 VAND. J. TRANSNAT'L L. 1, 45, 46, 107 (2004).

[248] Dennis T. Yokoyama, *You can't always use the Zippo code: The fallacy of a uniform theory of Internet Personal Jurisdiction*, 54 DEPAUL L. REV. 1147, 1150 (2005).

[249] Logically a State should be able to claim jurisdiction only if the offence has been committed, in part or in whole, in its territory; it must prove that a constituent element of the offence occurred in its territory, AKEHURST *supra* note 19, at 152. This is the formulation adopted in the Lotus case, *S.S. Lotus* (France v. Turkey) 1927 P.C.I.J. (Ser. A) No. 10 p. 23 & 30. Also at <www.geocities.com/hssph/Lotus.doc>.

the requirement of sufficient closeness between the alien and the state(s) in question. What here is termed "sufficient closeness"[250] seems equal to what Akehurst calls the 'Primary effect." Akehurst uses two factors to decide whether the effects are primary or secondary: (1) Are the effects felt in one State more direct than the effects felt in other States? (2) Are the effects felt in one State more substantial than the effects felt in other States? He argue this test fits the decided cases, in the sense that jurisdiction has been claimed in practice only by States where the primary effects of an act have been felt. This test – with its "requirement of directness" - enables jurisdiction to be exercised by one or two[251] States, which have a legitimate interest in exercising jurisdiction, but it prevents the exercise of jurisdiction by States with no legitimate interest.[252]

Clearly, it would be intolerable if jurisdiction could be exercised by every State where effects were felt, no matter how remote and slight those effects might be.[253]

A State is entitled to impose its ideology on its nationals and on all persons present in its territory; it is also entitled to oblige both categories of persons to take its side in its struggles against other States. But it is not entitled to make such demands on aliens living in foreign countries. Any such attempt would be incompatible with the political independence of the State of the aliens' nationality or residence. The protective principle of jurisdiction - the range of acts covered by the principle is not free from controversy - loses all validity when it is used, not to safeguard the political independence of the State claiming jurisdiction, but to undermine the political independence of

[250] SPANG-HANSSEN-2 *supra* note 8, at 365-366 & 382-418.

[251] The effects felt in two or more States may be equally direct or equally substantial; or direct but insubstantial effects in one State may be counter-balanced by indirect but substantial effects in another State. In such cases jurisdiction may be exercised by two or more States, but the number of States exercising jurisdiction is likely to be very small.

It is desirable to restrict jurisdiction to as small a number of States as possible, because there is no rule of international law against double jeopardy, and because an act which is lawful in one country may be a crime in another country-it is unfair to expose an individual to the conflicting requirements of legal systems in distant countries.

[252] AKEHURST *supra* note 19, at 154 and 198.

[253] AKEHURST *supra* note 19, at 192.

other countries.[254] In addition, the protective principle needs to be limited in the way that a State can claim jurisdiction only if the primary effect of the accused's action was to threaten that State.[255] If this is not so, a State can punish the editors of all the newspapers in the world for criticizing its government.[256] However, decided cases reveal examples of abuse.[257]

Under public international law the sufficient closeness is determined by objective facts, not by subjective or political views[258] by the state in question, for example whether the there is an interest of the forum state in providing a forum for its residents (or the plaintiff), the importance of the forum to the plaintiff's interest's in convenient relief , or the forum state's interest in adjudicating the dispute.

Litigation against an alien defendant should require a higher threshold than litigation against a citizen from a sister state in a Federal republic because important sovereignty concerns exist.[259] The international nature of the

[254] Spain passed in 2002 legislation authorizing judges to shut down Spanish sites and block access to U.S. webpages that do not comply with national laws. A report of 2002 found over 50% of racist sites were created in the U.S., Julia Scheeres, *Europeans Outlaw Net Hate Speech*, WIRED NEWS 9 November 2002 at <http://www.wired.com/news/business/0,1367,56294,00.html> (visited November 26, 2005).

[255] Nevertheless, the protective principle covers ground, which is not covered by the "effects" doctrine. For instance, if the accused counterfeits the currency of State A in State B, he cannot be tried in State A under the "effects" doctrine unless the counterfeit currency is put into circulation in State A; but the mere act of counterfeiting State A's currency, even if the counterfeit currency is never put into circulation, has a potentially adverse effect on State A, and this threat to State A justifies State A in claiming jurisdiction under the protective principle.

[256] AKEHURST *supra* note 19, at 159.

[257] AKEHURST *supra* note 19, at 158.

[258] MANN-2 *supra* note 54, at 15.

[259] It is of course a right for the federal republic to outline its own rules to decide which court inside the federal republic shall be allowed to exercise jurisdiction over an inhabitant of the federal republic - a question for the constitution of that federal republic. SPANG-HANSSEN-2 *supra* note 8, at 383-4. For the U.S. see *International Shoe Co. v. State of Washington*, 326 U.S. 310, 316 (US 1945)((The primary consideration in the jurisdictional inquiry is that of fundamental fairness to the defendant), *Rano v. Sipa Press, Inc.*, 987 F.2d 580, 599 (9th Cir. 1993), *Core-Vent Corp. v. Nobel Industries AB*, 11 F.3d 1482, 1489-90 (9th Cir. 1993)(A plaintiff seeking to hale a foreign citizen be-

Internet and the difficulty in identifying where transactions or statements are made, however, can give rise to grave difficulties in connection with for example intellectual property claims and arguments.[260] The overwhelming importance is to look at whether the alien defendant has expressly aimed or directed its conduct toward the forum.

Since the premise here is "pure online" incidents the only objective facts are the bits-transmission of either a message or information. As for messages (correspondence), the inquiry must be to look at which parties the message originally was sent to. If the receiver forward the message to a third-party without the consent of the original author, the latter cannot be held responsible. Further the inquiry must be into the facts contained in the message.

As for information in "pure online" incidents, this is achieved by the receiver connecting to a website. Thus, the inquiry must be looking into whether the author of the website has tried to aim special states by requiring the receiver to enter his zip-code or using a special access-code and into what content the website has, that is, what content and objectively opportunities the author offer on his website.

In this inquiry it should have no importance under what domain name the sender/author uses, as registrars of neither the top levels nor countries domain name require the name-applicant has any specific connection to either type of domain names.[261] Domain names should be regarded as they were originally intended, namely be pure and simple nicknames similar to the one used for telephone numbers. A domain name lacks a physical existence.[262] It is simply a unique identifier for a particular Internet site located on a particular computer. That computer may be located anywhere in the world and be unrelated

fore a court in the United States must meet a higher jurisdictional threshold than is required when the defendant is a United States citizen), *Outokumpu Engineering Enterprises, Inc. v. Kvaener Enviropower, Inc*. 685 A.2d 724 (Del. 1996); *OMI Holdings, Inc. v. Royal Insurance Company of Canada* 149 F.3d 1086 (10th Cir. 1998) and *OMI Industries, Inc, v. Kiekert AG*, 155 F.3d 254, 265 (3rd Cir. 1998).

[260] *Prince Plc v. Prince Sports Group Inc*., [1998] F.S.R. 21, 1997 WL 1104934 (English High Court of Justice (Chancery Div,) July 1997).

[261] On U.S. caselaw, see SPANG-HANSSEN-1 *supra* note 142, at 105-106;

[262] A domain names certificate supporting jurisdiction in registrar's country seems reasonable and close to that country.

to where the domain name is registered.[263]

Furthermore, use of either an international currency or international language on the website should have importance.[264] If a cybernaut wants to reach more than one country then he of cause has to use an international language, wherefore for example the U.S. cannot claim English language websites are targeting the U.S. As of 2005, 34 percent of the Internet users – or 8.2 percent of the world's population - have English as first language,[265] whereas the percentage that can use English – and do it on the Internet - is much higher.

The place of the server that hosts the website should neither determine the question of sufficient closeness.[266] A website seen on the screen of the receiver can have been build of information gathered from information stored on different servers placed around the world. Furthermore, of network administration reasons some information of often used websites will be stored as a copy on a proxy-server, which has no relation to the alien website author (or website host).

The content of a website's URL-address should neither be a factor as the website's information can be easily moved to another URL-address on a server on the other side of the globe. Sometimes this is done by a webhost-administrator – without the knowledge of the author/uploader of the information - of pure computer technical administrative reasons.

The fact that information on a website – except in the relatively insignificant number of cases where access-code are required – is accessible everywhere and for everybody does not in it self support such a closeness as required by public international law. The argument that a cybernaut should know that anything uploaded is accessible for everybody, wherefore jurisdiction can be exercised by any State with Internet access, is fundamentally wrong under the closeness requirement – or Akehurst's primary effect test – and it is certainly not fulfilling the reasonableness requirement under public

[263] *Easthaven Ltd. v. Nutrisystem.com Inc*., 2001 CarswellOnt 2878 para 25 (Ontario Superior Court of Justice, August 2001 - 00-CV-202854).

[264] On U.S. caselaw, see SPANG-HANSSEN-1 *supra* note 142, at 101-104;

[265] See Appendix A "Estimated evolution on Online Linguistic Population" in SPANG-HANSSEN-2 *supra* note 8, at 534.

[266] On U.S. caselaw, see SPANG-HANSSEN-1 *supra* note 142, at 107-110.

international law.

Therefore, the holding of the U.K. High Court, Queens Bench Division that an "internet publication takes place in any jurisdiction where the relevant words are read or downloaded"[267] is a violation of public international law as it allows jurisdiction equal to universal jurisdiction that can only be exercised in the few special cases supported by the international society (public international law). It shows the lack of understanding of how public international computer networks function. It would be more appropriate for the court to state that logging on to public international computer networks require special considerations. It is worth noting that the House of Lords - even though it had a good opportunity - avoided making any statement about the accessibility of information on the Internet. Maybe it had the same thoughts as U.S. justice Souter about deciding on the quickly changing technology, see above *Denver v. FCC*.[268]

The U.K. court should also consider the definition of "publish," which can mean: "to have one's work accepted for publication",[269] that is, not yet available for the public. Neither does a State have jurisdiction under public international law over people that use their constitutional right to give an expression that can be heard in the neighboring State. Furthermore, an author has not published something in a specific State just because a person brings an example of the publication into that State from another State. This is exactly what is happening on the Internet. The user, not the publisher, is deciding into what State the information is read or downloaded.

A website that does nothing but give information should not allow global jurisdiction or any kind of jurisdiction. Given the Internet speakers' inability to control the geographic location of their audience, expecting them to bear the burden of controlling the recipients of their speech may be entirely too much to ask.[270] The mere fact that websites can be accessed anywhere in the world does not mean that the law on the fact should regard the fact as being used everywhere in the world. It all depends upon the circumstances, particu-

[267] See above section III.D.2.
[268] Above note 204.
[269] Merriam-Webster's 11th Collegiate Dictionary and Oxford Talking Dictionary.
[270] Justice Sandra O'Connor in *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564, 122 S.Ct. 1700, 1714 (U.S. May 2002).

larly the intention of the website owner and what the reader will understand if he accesses the site.[271]

There are obvious advantages in attributing jurisdiction to the State where the facts occurred, and whose law has the closest connection with those facts.[272] Akehurst mentions that limitations also apply to laws conferring sovereign or prerogative rights on the State, for example tax laws can be applied only against people who have a close connection with the State concerned. What counts as a close connection will vary from context to context. If a foreigner visits a State for a couple of days, the State would be entitled to require him to register with the police, but not entitled to conscript him into the army.[273] Likewise, a State may expropriate property situated in its own territory; it may also expropriate property held by its citizens abroad although such legislation is unlikely to be enforced by the courts of other countries. But it would clearly be contrary to public international law for a State to pass such legislation concerning property held by foreigners abroad (the fact that such legislation will not be enforced abroad does not diminish its illegality). Akehurst points out that fortunately there seems to be no recorded example of such legislation.[274]

There does not seem any reason to change this pattern of a States' limitation just because information on the public international computer networks can be access from everywhere and by everyone. Global (or General) jurisdiction on basis of "pure online" is not acceptable by public international law. Specific jurisdiction on basis of "pure online" is only acceptable by public international law if there exists sufficient closeness in particular case. The opposite would allow plaintiff to forum shopping to an extent that has never been accepted by the international society. The starting point has to be the old maxim[275] that plaintiff must choose the jurisdiction in which the alien is located - a rule that should be cited by every court in every case involving "pure online" incidents; as should a remark that the issue in the case is inter-

[271] *R. v. 800-Flowers Trade Mark*, [2002] F.S.R. 12 para 47, 2001 WL, 2001] EWCA Civ 721483071 (English Court of Appeal, May 2001).
[272] AKEHURST *supra* note 19, at 175.
[273] AKEHURST *supra* note 19, at 179.
[274] AKEHURST *supra* note 19, at 180.
[275] "actor sequitur forum rei".

national.

Except for "pure online" incidents there does not exist anything similar with such a world wide reach and this require special treatment on the jurisdictional question. Global jurisdiction has never been allowed except in case of universal jurisdiction – and neither exchange of information or doing business comes close to the class of cases that under public international law allows universal jurisdiction.

The above mentioned U.S. case *Gator* held that defendant's virtual store on its website was "substantial, continuous and systematic." If one takes the numbers given in the decision it can be estimated that the online sales to the forum state was 1.96 million dollars (or 0.0096 percent of its total sales). This has by other courts been held not sufficient to exercise general jurisdiction.[276]

The court in Millennium Enterprises[277] defined "doing business over the Internet" as only such "business which conduct a significant portion of their business through ongoing Internet relationship," but did not allow exercise of general jurisdiction.

Assertions of global jurisdiction generate very high spillover effects. In the bricks and mortar world, it takes a great deal of resources to maintain a significant presence outside of one's home state. A "presence" such as a "virtual" presence on the Internet does not indicate a deliberate intention to enter that market. Accordingly, using Internet-based contacts to support global jurisdiction would greatly expand the number and type of defendants subject to global jurisdiction, as well as subject those defendants to a multitude of highly burdensome jurisdictional claims.[278] Global jurisdiction based exclusively on Internet presence creates more problems that it resolves, is not subject to discernable standards, and will surely add to the volume, if not the

[276] *Chiaphua Components Ltd. v. West Bend Comp*., 95 F.Supp.2d 505 (E.D.Va. 2000) at *6 and footnote 4. On cases involving the Internet and general personal jurisdiction, see further SPANG-HANSSEN-1 *supra* note 142, at 197-226.

[277] *Millennium Enterprises, Inc. v. Millennium Music*, 33 F.Supp.2d 907, 920 (D.Or. 1999).

[278] Allan R. Stein, *Personal Jurisdiction and the Internet: Seeing Due Process through the Lens of Regulatory Precision*, 98 Nw. U. L. Rev. 411, 437 (2004).

confusion, of jurisdictional analyses.[279]

As the content on a business website will change very often and, at least its sub-websites, nearly constantly it can be questioned whether the virtual online store is continuous and systematic. The content that a customer sees might be build together by content from servers around the world – or even from proxy servers – wherefore one cannot rightfully state that the online store is continuous – rather the website content changes often (sometimes all the time). On the other hand one can argue that any website or information will be accessible continuously and constant since it is hard to remove something from the Internet where several automatically website-archives also exists.

The global jurisdiction issue must turn on the evaluation of all of the defendant's activities in the forum state. Defendant's activities in the forum state, for purposes of global jurisdiction, must rise beyond the mere potential for marketing and sales that an interactive website may provide.[280] A single sale should not allow global jurisdiction as a purchase of a tourist in a foreign country does not allow the tourist's nation to exercise jurisdiction over the visited county's vendor. The inquiry must focus on whether the company's contacts are substantial, continuous and systematic for the forum.

An inquiry that taps into the quantum of business that the defendant does in the forum state is required. A website that targets residents of a particular state but fails to generate substantial revenue from that state should not subject the website operator to global jurisdiction. By the same token, a website that does not target the residents of a particular state but generates continuous and substantial revenue from that state's residents should suffice to establish global jurisdiction over the operator.

The problem with general or global jurisdiction and Cyberspace business is that if the terms qualifying for this are not very, very strict any online business will be under global jurisdiction with any court in the world. Thus, the courts must before they allow global jurisdiction think very thoroughly whether its reasoning can be copied by another State to also exercise global

[279] P. NANDA AND DAVID K. PANSIUS, LITIGATION OF INTERNATIONAL DISPUTES IN U.S. COURTS §1:31, LOID S 1:31 (August 2005).

[280] Dennis T. Yokoyama, *You can't always use the Zippo code: The fallacy of a uniform theory of Internet Personal Jurisdiction*, 54 DePaul L. Rev. 1147, 1194 (2005).

jurisdiction over the alien's online business.

Websites change all the time and thereby the online business. New software and new business practices evolve all the time, thus it is difficult to state that a business is having a certain custom that courts can rely on when they determine whether an alien online business is under global jurisdiction.

This makes any precedent or Stare Decisis theory work badly with the issue at hand, since it is more than likely the alien's online business - probably caused by new technology not older than 6 month - will have changed its habits and it's website before the next case comes to court. Thus, the new court cannot rely on the older decision(s) on the matter of that business' closeness with the forum.

It is a question of whether a website or Cyberspace facts alone should support global jurisdiction, since once a forum have declared foreign business using a website for having global jurisdiction in the state then the alien can be sued for any type of case it that foreign state. An a online business that declares it is not doing business with a certain forum anymore, should make it impossible for a court of that forum to exercise global jurisdiction in future.

It is not the intention of the international law on jurisdiction to allow all state's to decide global jurisdiction. This imply that a state cannot decide global jurisdiction on the content of a website's activity alone, since any court in the world should then be allowed to exercise global jurisdiction on the same basis; and anybody doing business online would then be under universal jurisdiction - and for any type of case.

3.4.2. Reasonableness

In international law, the principle of reasonableness appears unobjectionable, so long as it is understood that mere political, economic, commercial or social interests are to be disregarded when it comes to the weighting, which every test of reasonableness implies. Further, it is reasonableness in public international law that is decisive. In each case the overriding question is: Does there exist a sufficiently close legal connection to justify, or make it reasonable for, a State to exercise jurisdiction? Exercise of jurisdiction by more than one state may be reasonable, because public international law does not prohibit

concurrent jurisdiction over international criminal and civil matters.[281] However, a state should defer to the other state if that state's interest is clearly greater.[282] It is reasonable to require of any State that it acts in such a way that gives a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit.[283]

One area where global jurisdiction should be presumably impermissible involves non-commercial websites maintained by individuals, as it is unreasonable for a nation to assert global jurisdiction over a non-citizen residing outside of its borders.[284]

The only real limits to national regulation of the Internet are found in the internationally accepted principles of global jurisdiction. Here, the overriding limitation on whether a state can regulate a foreign Internet service or content provider is reasonableness. One scholar requires that if a commercial site does everything within its powers to limit for example offensive material, then the assertion of global jurisdiction lacks the element of reasonableness required to make such an assertion a legitimate exercise of state power.[285] But, out of consideration for the international society it would be more reasonable that the local community accepted aliens right to use the international network as they want and in stead locally made certain that the local community's own citizens locally was prevented from access to websites, which is not in accordance with that local community's laws.[286]

Akehurst points out that even when a State has legislative jurisdiction, the

[281] BROWNLIE *supra* note 13, at 309-310.

[282] REST-Foreign *supra* note 12, at § 403(3). See also REST-Foreign § 441 *supra* note 12, at and SPANG-HANSSEN-2 *supra* note 8, at Chapter 29.

[283] SPANG-HANSSEN-2 *supra* note 8, at 369-371 and 418-419. On some factors to consider on reasonableness, see 254-257.

[284] Walter C. Dauterman, *Internet Regulation: Foreign actors and local harms - At the crossroads of pornography, hate speech, and freedom of expressio*n, 28 N.C. J. Int'l L. & Com. Reg. 177, 219 (2002).

[285] *Id.* at 218.

[286] Henrik Spang-Hansen, *The earthly chaos in websites - question of jurisdiction and net-censorship* at <www.geocities.com/hssph/articles> (Translation of article *The jordiske kaos over websider – jurisdiktionsspørgsmål og netcensur*, KRITISK JUSS page 63-67 [Norwegian Law Journal "Critical Law"], No. 1-2/2001, Norway, ISSN 0804-7375).

State will still break international law if the content of its legislation is contrary to international law.[287] He notes that for international companies it would be intolerable if a large number of States claimed concurrent jurisdiction. The content of certain kind of law varies enormously from one State to another, and business cannot be carried on efficiently if it is subject to conflicting requirements from different States. As far as possible, therefore, restrictive business practices should be subject to municipal law but the number of States claiming jurisdiction should be as small as possible.[288]

By the same means it would be intolerable and unreasonable to require that because a business makes an online virtual store, it should comply with the law of all states wherefrom there is Internet access. The number of states allowed to have jurisdiction should be as small as possible.

As requirement of access-code to every website would slower the Net and irritate every cybernaut it would be unreasonable to require website authors to make force them to access-code if they want to prevent being under global jurisdiction.

Thus omission of password or access-code should not harm the alien cybernaut. In this respect, it is only by reference to motives that one can explain the exercise of jurisdiction over omissions.[289] As a general rule, no State is entitled to pass a law obliging people in other States to trade with it; such people may have legitimate reasons for not wishing to trade.[290] Taking the defendants' motives and intentions into account may add to the number of States entitled to exercise jurisdiction. However, even in such cases the number of States entitled to exercise jurisdiction should be small.[291]

Exercise of global jurisdiction because information is available on a website that can be read and downloaded from everywhere is without reason. The

[287] AKEHURST *supra* note 19, at 188.
[288] AKEHURST *supra* note 19, at 192.
[289] But even here some effects may be too indirect to justify jurisdiction, whatever the motives. For instance, if customers in State A refused to buy from a factory in State A owned by nationals of State B because they wanted to prevent remittance of profits to State B, it is submitted that the effect on B would be too indirect to justify jurisdiction, despite the customers' motives.
[290] AKEHURST *supra* note 19, at 200.
[291] AKEHURST *supra* note 19, at 201.

state in question must show it is reasonable to exercise jurisdiction over a specific "pure online" alien cybernaut on the specific issue and in that specific case.

3.5. Final Remarks

The public international computer network can only work if states does not make it into chaos – citizens wants to use it, they wants speed in the net for voice-IP, video, and games. They prefer it to be global with no censorship, rather than having the net slowed down because of national filters. Neither do they want the risk of allowing global jurisdiction, which indirectly advances world wide forum shopping to plaintiffs. A state are not allowed to exercise Global jurisdiction[292] – distinguished from Universal Jurisdiction - under public international law, which require a sufficient closeness (a close link) and reasonableness. This also imply, that a narrow community view[293] will only be acceptable under public international law as far as a statute or court decision does not reach outside the national border of the forum State.

Legislators must find other ways to legislate than software coding on devices on the public international computer networks – especially basic if the Internet Protocol has become customary international law wherefore it has to be obeyed by every state. They can choose to legislate on the hardware (nodes) inside their own country, but this will on the other hand prevent them from being a "full member" of the public international computer network with the thereof following disadvantages, and thus not offer "pipelines" for the public international computer network.

Maybe the time has come – as far as for "pure online" incidents - where Nations should give up making it possible for plaintiff to make forum shopping and return to the old basic rule, that is, that if a person wish to sue another cybernaut the plaintiff must go to the defendant's forum. E-mail communication and airplanes makes it easy and economically possible for a plaintiff to go to the defendant's forum. One can only hope the single con-

[292] Confer definition above in section 3.3.1.

[293] For example discussed by the U.S. Supreme Court in *Reno v. American Civil Liberties Union*, 521 U.S. 844, 877 (US, 1977).

sumer, who in practice often have no problem using the most advanced computer game, will be forced to learn that by login on to the Internet one has removed themselves from the local community's consumer protection and as a tourist has gone to a foreign nation, which most likely has different rules and laws that have to be read and studied - in stead of carelessly surfing the Internet and clicking links to new websites without reading the webpage's user conditions and realizing what part of the world they are dealing with.[294]

Today, customers are also tourist that travels around to far away places with totally different legislations from that of their home forum. Thus, customers in certain weeks of the year are used to be under foreign legislation – why not also let this be the case for pure online cross-border disputes!

[294] See *supra* note 232.

CHAPTER 4

The Zippo Sliding Scale-Method

Web site facts are important for a court's decision of whether to refer the case to a certain forum –

The Zippo decision is still the leading case – if the decision is used faithfully

By Henrik Spang-Hanssen

4.1. Introduction

In a great number of cases in the U.S. where a website has been one of the facts the plaintiff has tried to convince the court to exercise personal jurisdiction over the defendant based on the existence of the website. Thus, the question as to what kind of activity a website has to have for allowing exercise of jurisdiction has arisen in the courts.

Since the contents of a website can be seen by all cybernauts worldwide – unless it requires a password to get further than the homepage – a U.S. court determination on a certain website's activity ought to be the same in every court, because the technicality of the website is of course the same everywhere. The only two remaining questions would be whether or not another court would hold that a higher or lower level of activity was required for exercising personal jurisdiction in that other court; and whether that court

would find the particular website was aimed at the forum.[1]

Initially for those not acquainted with the U.S. rules of personal jurisdiction it should be mentioned that the upper limit of the jurisdiction rules over a non-resident has been made by the U.S. Supreme Court and divided into a General personal jurisdiction rule and a Specific personal jurisdiction. The later could be called an extraordinary jurisdiction rule. Further, should pointed out that U.S. courts when deciding the personal jurisdiction rule does not take any account to the subject matter discussion.

4.2. Als Scan, Inc. v. Digital Service Consultants, Inc., of June 2002

The June 2002 case *Als Scan, Inc. v. Digital Service Consultants, Inc.*[2] dealt with a question of first impression for the Fourth Circuit on whether a person electronically transmitting or enabling the transmission of information via the Internet to Maryland, causing injury there, subjects the person to the jurisdiction of a court in Maryland. The Circuit initially pointed out that applying the traditional due process principles requires some adaptation of those principles because the Internet is omnipresent. It remarked that to conclude as a general principle that a person's act of placing information on the Internet subjects that person to personal jurisdiction in each State in which the information is accessed, would mean that the defense of personal jurisdiction, in the sense that a State has geographically limited power, would no longer exist.

[1] The article is partly built on Chapter III of the book HENRIK SPANG-HANSSEN, CYBERSPACE JURISDICTION IN THE U.S.: THE INTERNATIONAL DIMENSION OF DUE PROCESS, especially 197-226 (Complex 5/01, Norwegian Research Center for Computers and Law, Oslo University 2001 - ISBN 82-7226-046-8 – US Congress Library 2003450386), free download from <www.geocities.com/hssph> [hereinafter SPANG-HANSSEN-1].

[2] *Als Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Circuit, June 2002)(The court held the Defendant did not select or knowingly transmit infringing photographs specifically to Maryland with the intent of engaging in business or any other transaction in Maryland, Rather, its role as an ISP was at most passive; and Defendants website was unrelated to Plaintiffs claim in the case, because the website was not involved in the publication of any infringing photographs, thus not directed its electronic activity specifically at any target in Maryland), *certiorari denied by* U.S. Supreme Court on January 13, 2003, 537 U.S. 1105 (S.Ct. 02-463).

The Fourth Circuit held that it would be to broad a interpretation of the minimum contacts test, if a plaintiff could argue that the Internet's signals are surrogates for the person and that Internet users conceptually enter a State to the extent that they send their electronic signals into the State, establishing those minimum contacts sufficient to subject the sending person to personal jurisdiction in the State where the signals are received. Otherwise, jurisdiction over persons would be universal, and notions of limited State sovereignty and personal jurisdiction would be eviscerated. Such a thought certainly would have been considered outrageous in the past when interconnections were made only by telephones. The Circuit also rejected to use the "stream-of-commerce" concept from *Asahi Metal Industry*[3] as this has never been adopted by the Supreme Court as the controlling principle for defining the reach of a State's judicial power.

Therefore, the court had to develop, under existing principles, the more limited circumstances when it can be deemed that an out-of-state citizen, through electronic contacts, has conceptually "entered" the State via the Internet for jurisdictional purposes.

For the use of deciding the question of specific personal jurisdiction[4] the court adopted the model developed in the *Zippo*-case[5] - see further below - which concluded 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." The Circuit held a State may, consistent with due process, exercise judicial power over a person outside the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

The court noted that under this standard, a person who simply places information on the Internet does not subject himself to jurisdiction in each State

[3] *Asahi Metal Industry Co., Ltd. v. Superior Court of California*, 480 U.S. 102 (U.S. (Cal) 1987).

[4] Specific personal jurisdiction requires purposeful conduct directed at the State and that the plaintiff's claim arise from the purposeful conduct.

[5] *Zippo Manufacturing Company v. Zippo Dot Com, Inc*., 952 F.Supp. 1119 (W.D. Pa. 1997) [hereinafter *Zippo*].

into which the electronic signal is transmitted and received. This standard is not dissimilar to that applied by the Supreme Court in *Calder v. Jones*.[6]

Further, the Circuit remarked that it was not prepared to obtain general jurisdiction over out-of-state persons who regularly and systematically transmit electronic signals into the State via the Internet based solely on those transmissions. Something more would have to be demonstrated, and the Circuit did not need to decide what that "something more" should be because of lack of information from the plaintiff.[7]

4.3. The Zippo case of 1997

In the *Zippo* case[8] the famous lighter company claimed a California company had misused plaintiff's trademark by using a website with the domain name "Zippo.com". Defendant Dot Com operated 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 moved for dismissal for lack of personal jurisdiction pursuant to Fed.R.Civ.P. 12(b)(2). Plaintiff claimed only specific personal jurisdiction, but did not claim general personal jurisdiction, thus not that defendant had substantial and continuous connections with the forum in which the court was presided.

Defendant's customers could fill out an on-line application that asked for a variety of information including the person's name and address. Payment was made by credit card over the Internet or the telephone. The application was

[6] *Calder v. Jones*, 465 U.S. 783 (U.S. (Cal) 1984).

[7] The *Zippo* case has also been positively discussed by the Fifth Federal Circuit in *Mink v. AAAA Development LLC*, 190 F.3d 333, 336 (5th Cir. (Tex), 1999), by Six Federal Circuit in *Neogen Corp. v. Neo Gen Screening, Inc*., 282 F.3d 883, 890 (6th Cir. (Mich) Mar. 2002) and *Bird v. Parsons*, 289 F.3d 865, 875 (6th Cir. (Ohio) May 2002), by 9th Federal Circuit in *Cybersell, Inc. v. Cybersell, Inc*., 130 F.3d 414, 418 (9th Cir. (Ariz.) Dec 1997) and by 10th Federal Circuit in *Soma Medical International v. Standard Chartered Bank,* 196 F.3d 1292, 1296 (10th Cir. (Utah) Dec 1999).The Zippo case has been cited by the D.C. Federal Circuit in *Gorman v. Ameritrade Holding Corp*., 293 F.3d 506, 513 (D.C.Cir. June 2002).

[8] The case is quoted relativity thoroughly here as for the readers that have no access to American law reviews

then processed and the subscriber was assigned a password which permitted the subscriber to view and/or download Internet newsgroup messages that was stored on the Defendant's server in California.

In this case the court remarked[9] that the Internet makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages.

The court found that the cases were scant. Nevertheless, the court's review of the available cases and materials revealed 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.

This *sliding scale* is consistent with well-developed personal jurisdiction principles. *At one end* of the spectrum are situations where a defendant *clearly does business* over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. [ ] *At the opposite end* are situations where a defendant has *simply posted information* on an Internet Website which is accessible to users in foreign jurisdictions. A passive Website that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. [ ] *The middle ground* is occupied by interactive Websites where a user can exchange information with the host computer. 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 Website. [ ] Traditionally, when an entity intentionally reaches beyond its boundaries to conduct business with foreign residents, the exercise of specific jurisdiction is proper. [ ] Different results should not be reached simply because business is conducted over the Internet. (Author's emphasizing. Citations omitted).[10]

[9] *Zippo supra* note 5, at 1123-1124.

[10] P. NANDA AND DAVID K. PANSIUS, LITIGATION OF INTERNATIONAL DISPUTES IN U.S. COURTS §1:29 holds the more critical question are: (1) what is the website's function; (2) what is that function as it relates to the Claim; and (3) absent such a relation, is the

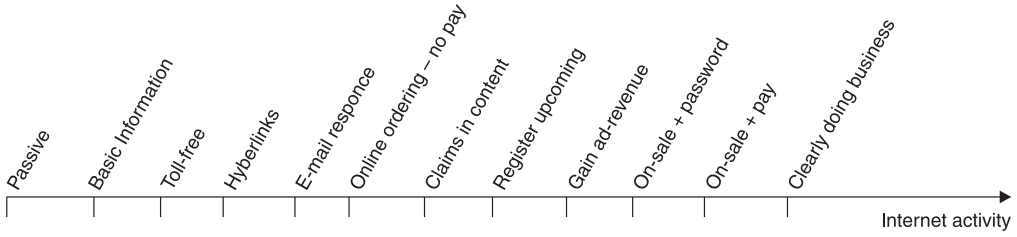

Table 4.1 – Zippo's Interactive Scale

The court noted that it was not dealing with an Internet advertising case in the line of *Inset Systems*[11] and *Bensusan*[12], because defendant had not just posted information on a Web site that was accessible to Pennsylvania residents who were connected to the Internet. This was not even an interactivity case in the line of *Maritz*[13], because defendant Dot Com had done more than create an interactive Web site through which it exchanged information with Pennsylvania residents in hopes of using that information for commercial gain later.[14]

The court noted that it was not being asked to determine whether Dot Com's Web site alone constituted the purposeful availment of doing business in Pennsylvania.

It held that is was dealing with a "doing business over the Internet" case in the line of *CompuServe*[15], because the court was being asked to determine whether Dot Com's conducting of electronic commerce with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania. It concluded that it did. Dot Com had contracted with approximately 3,000 individuals and seven Internet access provider s in Pennsylvania. The

function so intrusive or pervasive as to otherwise support the exercise of jurisdiction, LOID S 1:29 (August 2005).

[11] *Inset Systems, Inc. v. Instruction Set*, 937 F.Supp. 161 (D.Conn. 1996) .

[12] (the "Blue Note" case) *Bensusan Restaurant Corp., v. King*, 937 F.Supp. 295 (S.D.N.Y.1996). The lower court decision, which was *affirmed by* the Circuit court with a different reasoning, see 126 F.3d 25 (2nd Cir. 1997).

[13] *Maritz, Inc. v. Cybergold, Inc*., 947 F.Supp. 1328 (E.D.Mo. 1996) .

[14] *Zippo supra* note 5, at 1126.

[15] *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996) .

intended object of these transactions had been the downloading of the electronic messages that form the basis of this suit in Pennsylvania.

The intended object of these transactions had been the downloading of the electronic messages that form the basis of this suit in Pennsylvania. The court found necessary forum-related activities were numerous or significant enough to create a "substantial connection" with Pennsylvania and defendant's contacts were "deliberate and repeated even if they yielded little revenue."

It also concluded that the cause of action arose out of Dot Com's forum-related conduct and remarked that the Third Circuit has stated that "a cause of action for trademark infringement occurs where the passing off occurs.

4.4. Web-sites (activity level catalog) – U.S. Cases

Many cases especially since the 1997 *Zippo*[16] case, when determining the question of personal jurisdiction in connection with websites, in the published decision have reviewed thoroughly the contents of the website in question.[17] A very large number of cases have made a name-label-categorizing the website. Some have used a three-grouping of the interactivity.[18] Sometimes the courts have given the website extensive attention and the decisions contained extensive discussions on the website, whereas, other facts have only been discussed superficially.

It is worth noting that the court in *Zippo* not once in its decision used words like "group" or "categorize," or derivation hereof. What the *Zippo* case

[16] *Zippo supra* note 5, at 1123-1124.

[17] The court in *Winfield Collection, Ltd. v. McCauley*, 105 F.Supp.2d 746, 749 (E.D.Mich. 2000) found that the proper means to measure the site's "level of interactivity" as a guide to personal jurisdiction remained unexplained. "The distinction drawn by the *Zippo* court between actively managed, telephone-like use of the Internet and less active but "interactive" websites is not entirely clear to this court." The court in *Metcalf v. Lawson*, 2002 WL 1369639 (N.H. June 2002) did not find the Zippo test useful as this test is based on a defendants web site and the defendant in the actual case only had conducted transaction through an Internet auction site, eBay.

[18] *See* for example *Blackburn v. Walker Oriental Rug Galleries, Inc*., 999 F.Supp 636, 638 (E.D.Pa. 1998), and *Kubik v. Route* 252, Inc., 762 A.2d 1119, 1124 (Pa. Super. 2000).

used are words like "level" and "scale," which clearly indicate the *Zippo* case as for the issue of websites activity had a normal mathematic point of view, which is a scale from zero to either a fixed point or infinite.[19] The *Zippo* case chose the first alternative and called this highest scale-point "clearly doing business.[20] When using a scale ones talk about points on a scale and not of an "intermediate" or "middle" group. The Zippo case further talked about a "gliding" scale, which rule out any grouping.

However, a research of cases shows that the courts use various definitions, terms and levels for similar facts in a website. Based on a research[21] of nearly

[19] Webster (Merriam-Webster's Collegiate Dictionary 10th Edition) defines "scale" as: something graduated especially when used as a measure or rule; a series of marks or points at known intervals used to measure distances; a graduated series or scheme of rank or order. Further Webster defines "group" or "categorize" as - Group: two or more figures forming a complete unit in a composition; a number of individuals assembled together or having some unifying relationship; an assemblage of objects regarded as a unit. - Categorize: to put into a category, which is defined as a division within a system of classification, which is defined as a systematic arrangement in groups or categories according to established criteria. This may be reasoned by the fact as the U.S. Supreme Court stated in *Reno v. ACLU*, 521 U.S. 844, 870 (U.S.. 1997): "the content on the Internet is as diverse as human thought."

[20] Businesses like auctions house eBay are not considered offering or selling items on its web sites and cannot be held liable for actions done on its web sites because of 47 U.S.C. § 230, *see Zeran v. America Online, Inc*., 129 F.3d 327 (4th Cir. (Va) 1997), *cert. denied* 524 U.S. 937 (U.S. 1998) and *Gentry v. eBay, Inc*., 121 Cal.Rptr.2d 703, 2002 WL 1371153 (Cal.App.4 Dist., June 2002).

[21] On basis of the cases mentioned in Chapter III, D.b and the courts activity-name-label one can outline an activity-line for Trade/Commercial sites and tables I-II as shown in Chapter III.D.a of SPANG-HANSSEN-1 *supra* note 1. In making the presentation of the cases in the tables it was considered to use a *computerized analyze research model* like SARA (see Jon Bing, *Modeller av Rettslige Avveininger med et eksempel fra Norsk Interlegal Rett*, TIDSSKRIFT FOR RETTSVITTENSKAB 1985.395 [Models of legal balancing Process with examples from Norwegian Interlegal Law, Periodical for Legal Science (Oslo)]) or Taxman (see L. Thorne McCharty, *Reflections on Taxman: An experiment in artificial intelligence and legal reasoning*, 90 HARVARD LAW REVIEW 837. See also Colin Tapper, *The "Oxford Experiments", Prediction of Juridicial Decisions*, COMPUTERS AND THE LAW 232-251 (London 1973)).However, use of such models is limited to a few basic parameters and this basic requirement does not seem to be obtainable, because the types of contents on a website are to many-sided. The conclusion of

every published case from 1995 until 2001 where the contents of the website have been heavily quoted in the court's decision[22] and where website activity has been discussed in connection with the determination of whether or not personal jurisdiction could be exercised in a U.S. state over a non-resident defendant the table below can be drawn. [23]

Table on cases that exercises jurisdiction and where web-content has been referred thoroughly in decision (as of December 2000):

the following research of case law also imply it would impossible to make a computerized analyze as there can't be set up any necessary equation.

[22] The web site's content of the cases is listed in Chapter III, D.b. in SPANG-HANSSEN-1 *supra* note 1.

[23] This table is an extract of tables from Chapter III.D, id.

Table 4.2: Cases which exercises jurisdiction and where web-content has been referred thoroughly in decision

Case Name	Courts Classification	Basic company information	Basic incl. Parent or subsidiary	Advertising incl phone & address	+ e-mail address	Products	Prices	Toll-free number noted on site	Hyperlinks	Other interactive features	E-mail response	On-line ordering – No payment	Claims incl. In content	Registering for upcoming service	Gain advertising revenue	On-sale & payment after issue account	On-line sale & payment
Intern. Star Registry v Bowman-Haight Vent.	B												**S***				**S**
Colt Studio v Badpuppy Enterprise [650]	B												**S**				**S**
Thompson v Handa-Lopez	B																**S**
Digital Equipment v AltaVista	B												**S**		**S**		
Inset System v Instruction	B			**S**				**S**					**S***				
Zippo Mfg. v Zippo Dom Com	B												**S***			**S**	
Minnesota v Granite Gate Resort	B													**S**			
Maritz v CyberGold	(B)												**J***	**J**	**J**		
American Eyewear v Peeper's Sunglasses	B												**S**				**S**
Stomp v NeatO	B												**S**				**S**
Tech Heads v Desktop Service Center	B												**S***				**S**
Quokka Sport v Cup International	(B)												**S***				**S**
CompuServe v Patterson	(B)												**S**		**S**		
Northern Light Tech. v Northern Light Club	(B)												**S***		**S**		
Campell v American International Group	(I)		**J**	**J**		**J**											
Bochan v Harris	I																**G**
Hasbro v Clue computing	I				**S**	**S**							**S***				
Bancroft & Masters v Augusta National	P			**S**									**S***				

Note: P – passive. A bracket means the court have used other wording or none for classification
I – interactive. A bracket means the court have used other wording or none for classification
B – Doing business. A bracket means the court have used other wording or none for classification
N – No jurisdiction
Bold – Jurisdiction
*- Case involving Defendants domain name and Plaintiff's mark
Black background – cases that cannot be classified as doing business on-line

If one from the above table deletes cases involving Defendants domain name and Plaintiff's mark, and cases that should not be classified as doing business on-line, one gets the following table:

Table 4.3

Case Name	Courts Classification	Basic company information	Basic incl. Parent or subsidiary	Advertising incl phone & address	+ e-mail address	Products	Prices	Toll-free number noted on site	Hyperlinks	Other interactive features	E-mail response	On-line ordering – No payment	Claims incl. In content	Registering for upcoming service	Gain advertising revenue	On-sale & payment after issue account	On-line sale & payment
Colt Studio v Badpuppy Enterprise	B												S				S
Thompson v Handa-Lopez	B																S
Digital Equipment v AltaVista	B												S		S		
Minnesota v Granite Gate Resort	B													S			
American Eyewear v Peeper's Sunglasses	B												S				S
Stomp v NeatO	B												S				S
CompuServe v Patterson	(B)												S			S	
Bochan v Harris	I																G

International Star Register of Illinois v. Bowman-Haight Venture, Inc., 1999 WL 300285 (N.D.Ill. 1999).
Colt Studio, Inc. v. Badpuppy Enterprise, 75 F.Supp.2d 1104 (C.D.Cal. 1999).
Thompson v. Handa-Lopec, Inc., 998 F.Supp. 738 (W.D.Tex. 1998).
Digital Equipment Corp. v. Altavista Technology, Inc. 960 F.Supp. 456 (D.Mass. 1997).
Inset Systems, Inc. v. Instruction Set, 937 F.Supp. 161 (D.Conn. 1996).
State of Minnesota v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn.App. 1997).
Maritz, Inc. v. Cybergold, Inc., 947 F.Supp. 1328 (E.D.Mo. 1996).
American Eyewear, Inc. v. Peeper's Sunglasses and Accessories, Inc., 106 F.Supp.2d 895 (N.D.Tex. 2000).
Stomp, Inc. v. NeatO, LLC., 61 F.Supp.2d 1074 (C.D.Cal. 1999).
Tech Heads, Inc. v. Desktop Service Center, Inc., 105 F.Supp.2d 1142 (D.Or. 2000).
Quokka Sport, Inc. v. Cup International Ltd., 99 F.Supp.2d 1105 (N.D.Cal. 1999).
CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. (Ohio), 1996).
Northern Light Technology v. Northern Lights Club, 97 F.Supp.2d 96 (D.Mass. 2000).
Campbell v. American International Group, Inc., 976 P.2d 1102 (Okla. Ct. App. Div.2, 1999).

Of these cases only *Minnesota v. Granite Gate Resort* and *Bochan v. Harris* falls outside the pattern where courts require a plaintiff to show evidence that the defendant actually have sold or given online support through the website. In the first case the defendant had set up a website but not started to do the business to forum residents. In the latter, there was no evidence of sales to the forum state.

An overwhelming part of the cases follow the pattern that one does not subject himself to the jurisdiction of the courts in another state simply because he maintains a website which residents of that state visit. However, one who uses a website to make sales to customers in a distant state can thereby become subject to the jurisdiction of that state's courts.[24]

The court in *ESAB* found decisions holding jurisdiction based solely on the maintenance of a website was wholly unpersuasive.[25] The court in *Barrett* noted, that [n]ot only does the weight of the authority favour the rationale that a "passive" website is insufficient to trigger jurisdiction, but we believe that such decisions comport with the traditional concept of personal jurisdiction where merely fortuitous contact is insufficient.[26]

As for the level activity on a website, a "passive" [27] website is mainly what the courts refer to as websites only containing information and advertisements.[28] The court in *International Star Register of Illinois* defined this type of website as those in which there is "no further communication with potential customers via the Internet" than the defendant's posting of information on the Internet. They are "websites that merely provide information or

[24] *National Football League v. Miller d/b/a NFL Today*, 2000 WL 335566 (S.D.N.Y. 2000) *quoting Bensusan Restaurant Corp. v. King*, 937 F.Supp. 295 (S.D.N.Y.1996) *affirmed partly by* 126 F.3d 25 (2d Cir. 1997) and *Bochan v. La Fontaine*, 68 F.Supp.2d 692, 701 (E.D.Va. 1999).

[25] *ESAB Group, Inc. v. Centricut, LLC*, 34 F.Supp.2d 323 at FN4 (D.S.C., 1999).

[26] *Barrett v. Catacombs Press*, 44 F.Supp.2d 717, 727 (E.D. Pa. 1999).

[27] Passive: Not active or operating; Synonym: inactive (Merriam-Webster On-line Dictionary, visited January 22, 2001).

[28] This definition was also used by the Court of Appeal for Ontario in *Pro-C Ltd. v. Computer City, Inc*. 2001 CarswellOnt 3115, 149 O.A.C. 190, 55 O.R. (3d) 577 (Eng.), 55 O.R. (3d) 583 (Fr.), 205 D.L.R. (4th) 568, 14 C.P.R. (4th) 441 (Ontario Court of Appeal for - No. C34719, Sep. 2001).

advertisements without more."[29] In *JB Oxford Holdings, Inc. v. Net Trade Inc*.[30] the court in footnote 9 defined a "passive" site as a website "where 'surfers' simply view advertisements for products and services." This seems to be a reasonable definition for the natural passive end of an activity-level-scale.

Yet some decisions[31] have not followed such a definition, but have extended the passive level to also include websites where a user has corresponded with the owner of the website, for example clicked an e-mail-icon and joined a list for information on future products. Such activity is definitely using "further communication" methods as defined in *Reno-1*, Fact-Finding number 22.[32] In *Bancroft & Masters, Inc.*[33] the 9th Circuit extended the type of a passive website to be where for example "consumers could not use it to make purchases." In *Campbell*[34], where the website should have been labeled passive, the court deemed it instead to be aggressively marketing, and allowed exercise of jurisdiction. The same has been said about the case, *Inset Systems*[35] that exercised jurisdiction only on the basis of a website, which was as passive as anyone can image.

The courts have neither agreed upon a definition of the natural other end of the scale, which the *Zippo* court named "clearly doing business." Some cases use the term, "commercial," to mean on-line-ordering without payment done on-line.[36] Other courts only use the term for sites where ordering and

[29] *International Star Registry of Illinois v. Bowman-Haight Ventures, Inc*., 1999 WL 300285, at *4 & *5 (N.D.Ill. May 6, 1999 - No. 98 C 6823) .

[30] *JB Oxford Holdings, Inc. v. Net Trade Inc*., 76 F.Supp.2d 1363 (S.D.Fla. 1999).

[31] *See* for example *Desktop Technologies, Inc. v. Colorworks Reproduction & Design, Inc.*, 1999 WL 98572 (E.D.Pa. 1999); *Grutkowski v. Steamboat Lake Guides & Outfitters, Inc.*, 1998 WL 962042 (E.D.Pa. 1998).

[32] *American Civil Liberties Union (ACLU) v. Reno*, 929 F.Supp 824, 834 (E.D.Pa. 1996) .

[33] *Bancroft & Masters, Inc. v. Augusta National, Inc*., 223 F.3d 1082 (9th Cir. (Cal), 2000). The court in *Meyers v. Bennett Law Offices*, 238 F.3d 1068 (9th Cir. (Nev), 2001) quoted its decision in Bancroft and explained the expression "something more" was equal to "express aiming" in the *Calder* case.

[34] *Campbell v. American International Group, Inc*. 976 P.2d 1102 (Okla. Civ. App. 1999) .

[35] *Inset Systems supra* note 11, at 165.

[36] For example *Decker v. Circus Circus Hotel*, 49 F.Supp.2d 743, 748 (D.N.J. 1999).

payment can both be done on-line.[37] The later seems to be what rightly should be named "clearly doing business" on-line. The court in *Standard Knitting, Ltd. v. Outside Design, Inc*.[38] characterized defendants website as "fully interactive" and one through which business is conducted with residents of foreign jurisdictions, including Pennsylvania. The court in *Citigroup Inc. v. City Holding Co*.[39] remarked that it was "not clear that the transaction could actually be consummated on line, a scenario which [would] bring this case out of the middle category and into the category of a business that clearly does business over the Internet in New York."

Some courts have chosen to look beyond the degree of interactivity provided by the website. Instead they emphasized the degree to which the defendant actually used its website to conduct commercial or other types of activity with forum residents.[40]

As for the highest interactivity level of the scale, the court in *Millennium* emphasized that, the capability of selling through a website does not constitute "doing business" over the Internet, which could otherwise confer personal jurisdiction almost as a matter of course. This is in order with the overwhelming cases requiring evidence of actual contact between the defendant and the forum state through the website. The *Millennium* court defined "doing business over the Internet" as only such "businesses which conduct a significant portion of their business through ongoing Internet relationships; for example, by entering into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet."[41] This definition of "doing business over the Internet," requiring a "significant portion" or "repeated transmission," seems on the other hand very limited and nearly requiring the same as if exercising general personal jurisdiction.

[37] For example *Stomp, Inc. v. NeatO, LLC*., 61 F.Supp.2d 1074 (C.D.Cal. 1999) and *Sports Authority Michigan, Inc. v. Justballs, Inc*., 97 F.Supp.2d 806 (E.D.Mich. 2000).

[38] *Standard Knitting, Ltd. v. Outside Design, Inc*., 2000 WL 804434 at *5 (E.D.Pa. 2000).

[39] *Citigroup Inc. v. City Holding Co*., 97 F.Supp.2d 549 at footnote 8 (S.D.N.Y. 2000). *See* also *National Football League supra* note 24, at *1.

[40] *Dagesse v. Plant Hotel NV*, 113 F.Supp.2d 211 at *9 (D.N.H. 2000).

[41] *Millennium Enterprises, Inc. v. Millennium Music. LP*, 33 F.Supp.2d 907, 920 (D.Or. 1999).

The court in *Chiaphua Components Ltd. v. West Bend Comp*.[42] – rejecting jurisdiction - used a similar limited definition and only found the interactive website in question to fit for the intermediate level even though defendant's website allowed visitors to make purchases, albeit not of the disputed water distillers. The actual sales with the forum were for 1997 $3,934,768, or 1.75% of total sales, to which the court noted that "[a]lthough a relatively small percentage of the overall sales of the corporation, it is difficult to conclude the sales are de minimus." The *Molnlycke* court, which rejected general jurisdiction, emphasized the website was "not central to defendants business" even though a small percentage of income was deriving from the forum state.[43] *Robbins v. Yutopian Enterprises* held forty-six Internet transactions during a 10 ½ month period were not enough.[44] The D.C. Circuit court in *Gorman v. Ameritrade* pointed out that the website allowed defendant stockbroker to engage in real-time transaction with the forum's residents while they sit at their home or office computers in the forum state and permitted such transactions to take place 24 hours a day to a degree that traditional foreign corporations never could even approach, thus the web site made it possible for defendant to have continuous and systematic contacts with the forum. The appeal court rejected to exercise general jurisdiction because of lack of facts on the frequency and volume of defendants transaction with the forum's residents.[45]

No court has defined "clearly doing business" through a website as equal to the requirement allowing the exercise of general personal jurisdiction, that is substantial, continuous and systematic contacts with the forum state. The *Zippo*-court speaks only of a gliding scale between cases where a defendant "clearly" does business over the Internet and cases only involving a website that does little more than make information available to those who are interested in it, which the court defined a "passive website".

[42] *Chiaphua Components Ltd. v. West Bend Comp*., 95 F.Supp.2d 505 (E.D.Va. 2000) at *6 and footnote 4.

[43] *Molnlycke Health Care AB v. Dumex Medical Surgical Products Ltd*., 64 F.Supp.2d 448, 452-453 (E.D.Pa. 1999).

[44] *Robbins v. Yutopian Enterprises, Inc*., 202 F.Supp.2d 426 (D.Ma. May 2002) at *4.

[45] *Gorman v. Ameritrade, 293 F.3d 506* at FN9. The court did not consider whether the assertion of personal jurisdiction was "reasonable"

Between these two outer points, the courts have used various characterizations that contradict one another and do not fit into anyone pattern. For example, a website allowing users to make hotel reservations in *Decker v. Circus*[46] was characterized as "commercial," while the court in *Dagesse v. Plant Hotel NV*[47] characterized such a website as not being used to do business or otherwise interact with the forum states residents. The court in *Hurley v. Cancun Play Oasis International Hotels*[48] characterized a similar website as having an interactive quality beyond a "passive website," whereas the court in *Weber v. Jolly Hotel*[49] characterized such a site as "passive".[50]

Some cases in making its determination of jurisdiction on the basis of Cyberspace have used the decision in Zippo.com[51] as a reference to a three-part-grouping consisting of "passive," interactive, and "clearly doing business" websites. Some have made other kind of groupings.[52] Yet, a three-part-

[46] *Decker v. Circus supra* note 36, at 748.
[47] *Dagesse v. Plant Hotel NV*, 113 F.Supp.2d 211 (D.N.H. 2000).
[48] *Hurley v. Cancun Play Oasis International Hotels*, 1999 WL 718556 (E.D.Pa. 1999).
[49] *Weber v. Jolly Hotels*, 977 F.Supp 327, 333 (D.N.J. 1997).
[50] In a similar case in *Romero v. Holiday Inn*, 1998 WL 961384 (E.D.Pa., 1998) held the court the website activity consisting of Internet reservations was not additionally significant as where toll-free telephone reservations are offered. Like "800" number service, an Internet connection allows a consumer to contact a hotel chain for reservations directly and without charge. The distinction of using a computer hooked to a telephone/data line is not relevantly different from using a handset connected to that same line; one is in writing and one is by voice--a distinction without difference in this context. So also, web-site reservations, a more modern version of toll-free reservations, do not change the result. *Pebble Beach Company v. Caddy*, 2006 WL 1897091, --- F.3d --- (9th Cir. July 2006) (Held British Bed and Breakfast passive website with plaintiff's domain name did not aim neither California nor the U.S.).
[51] *Zippo supra* note 5, at 1119.
[52] *Weber v. Jolly Hotels* at 333: "The cases dealing with [the] issue [of Internet and personal jurisdiction] can be divided into three categories." *See also Blackburn v. Walker Oriental Rug Galleries, Inc*., 999 F.Supp 636, 638 (E.D.Pa. 1998) and *Hurley v. Cancun Playa Oasis International Hotels*, 1999 WL 718556 at *2 (E.D.Pa. 1999).
In *ACLU v. Reno*, 31 F.Supp.2d 473, 486 (E.D.Pa. 1999) an expert divided websites into five general business models:
(1) the Internet presence model, which involves no direct sales or advertising but is used by a business to raise customer awareness of the name and products of the Website operator,

grouping is not correct considering the statutes on U.S. jurisdictional questions. Merely categorizing a website as interactive or passive is not conclusive of the jurisdictional issue.[53]

The court in *CoolSavings.com* had difficulty using such a three-part categorizing and held that the case did not fit any of the categories. The court did not think it was productive to try to "jam" the case into any categorizing-group. It found it unnecessary for the determination of whether or not personal jurisdiction could be exercised.[54]

The 14th (or 5th) Amendment of the U.S. Constitution and the long-arm statutes only authorize two alternatives – not three. Either a fact support for jurisdiction or it does not. The obvious, pointed out by the *Zippo* court, is, that either the "level of interactivity and commercial nature of the exchange of information that occurs on the Website" is sufficient to exercise personal jurisdiction or that it is not. Therefore, either the Cyberspace related facts alone is enough for finding personal jurisdiction, or it is not. There are no in-betweens. In *Origin Instruments Corp.*[55] the court found the interactivity on the website was not enough and noted: "Thus, the court must determine whether Defendant has done 'something more' that when combined with its website would establish that it is amenable to personal jurisdiction."

"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"[56]. Or as the U.S. Supreme Court has stated: the determination on whether minimum contacts exist "is one in which

(2) the advertiser supported or sponsored model, in which nothing is for sale, content is provided for free, and advertising on the site is the source of all revenue,
(3) the fee based or subscription model in which users are charged a fee before accessing content,
(4) the efficiency or effective gains model, by which a company uses the Web to decrease operating costs, and
(5) the online storefront, in which a consumer buys a product or service directly over the Web.

[53] *ESAB Group supra* note 25, at 330.
[54] *CoolSavings.com, Inc. v. IQ.Commerce Corp*., 53 F.Supp.2d 1000, FN3 (N.D.Ill. 1999).
[55] *Origin Instruments Corp. v. Adaptive Computer Systems, Inc*., 1999 WL 76794 (N.D.Tex. 1999).
[56] *Zippo supra* note 5, at 1124.

few answers will be written 'in black and white' The greys are dominant and even among them the shades are innumerable."[57] Although business is now transacted using modern devices, the established notions of due process and fair play, as expressed by Constitutional Due Process requirements, work well to determine whether an individual has established minimum contacts with a state sufficient for the state to exercise jurisdiction.[58] Until transactions with [forum] residents are consummated through [a] defendants' Website, defendants cannot reasonably anticipate that they will be brought before [the forums'] court, simply because they advertise their products through a global medium which provides the capability of engaging in commercial transactions.[59]

Some cases have referred to the *Zippo* or *Cybersell* cases and ordered special requirement for "something more" facts for allowing jurisdiction in Cyberspace cases.[60] Such cases are labeled casual as passive respectively interactive. Yet as the *Zippo* case rightfully points out, the vital examination in relation with Cyberspace-facts is of the "activity that an entity conducts over the Internet" or "the exchange of information that occurs on the Website."[61]

Some courts have quoted the *Zippo* case as requiring "something more" in other respects. Yet, the *Zippo* court simply stated that because a website that does little more than make information available to those who are interested in it - a "passive website" – there has to be something else, that is, other useful facts than Cyberspace activity to give ground for exercising personal jurisdiction. However, the case is no different from any other case when courts rely on a bunch of facts that in unison lead to the court exercising jurisdiction. In such cases, one can wonder why the courts give so much attention to the

[57] *Kulko v. California Superior Ct*., 436 U.S. 84, 92 (U.S. (Cal), 1978).

[58] *Precision Laboratory Plastic, Inc. v. Micro Test, Inc*., 981 P.2d 454, FN6 (Wash. Ct. App.Div.2, 1999).

[59] *Millennium supra* note 41, at 923.

[60] *For example McMaster-Carr Supply Company v. Supply Depot, Inc*., 1999 WL 417352 at *4 (N.D.Ill. 1999) "the something more…the act beyond just establishing the website that makes it reasonable" and *Nissan Motor Co., Ltd. v. Nissan Computer Corporation*, 89 F.Supp.2d 1154, 1159 (C.D.Cal., 2000) *affirmed by* 246 F.3d 675 (9th Cir. (Cal), 2000) "In the Internet context,…a passive website does not itself subject the defendant to personal jurisdiction… there must be 'something more'."

[61] *Zippo supra* note 5, at 1124.

website in the decision.

The courts attempt to categorizing a certain website is of limited value since a website's categorizing in one forum often may be different from other courts because it is the website's targeting-place that determines the forum courts fix of the activity-level.[62] A website may be very interactive for example in areas covering Zip-code numbers accepted by defendant and passive outside such areas, because the defendant will not do business with residents outside the Zip-code numbers. *Coastal Video Communication v. Staywell Corp* which rejected general jurisdiction noted the first requirement for exercising jurisdiction is that to find that an interactive website has the potential to reach a significant percentage of the forum state's population.[63] *Robbins v. Yutopian Enterprises* noted that the fact that a website operated from a foreign jurisdiction is available for access by residents of the forum state, and contains advertising for the defendant's goods or services and takes orders over a clearly active website, is not sufficient to subject the operator to the general jurisdiction of the forum's courts.[64]

It should also be emphasized that even though a website clearly seems to do business, the court must also be presented with evidence that the website is under the control of the defendant, due to the fact that the website technology permits the use of megatags,[65] which increase the likelihood that an Internet user who enters a search request on an Internet search engine will be directed to other sites than the "original" website.

Regarding the strictly non-business-content on a website or the other communications methods mentioned in the *Reno-2* case,[66] such as defama-

[62] *Schnapp v. McBride*, 64 F.Supp.2d 608, 612 FN9 (E.D.La. 1998).

[63] *Coastal Video Communications, Corp. v. Staywell Corp*., 59 F.Supp.2d 562, 571 (E.D.Va. 1999).

[64] *Robbins v. Yutopian Enterprises, Inc*., 202 F.Supp.2d 426 at *4 (D.Ma. May 2002).

[65] When a person "surf" the Internet using a "search engine" the latter matches the surfers inputted "keywords" to webpage domains, text and "metatags". Megatags are HTML codes assigned to a particular webpage by its creator that are intended to describe the contents of the web page.
Although the metagtags assigned to web pages assist keyword searches, the metatags do not necessarily appear in the text of a website that is a hit.

[66] *Reno v. American Civil Liberties Union (ACLU)*, 521 U.S. 844, 850-857 (U.S. (Pa), 1997).

tory statements, U.S. courts have used another pattern. These cases can be interpretated using the *Calder* effect test on the defamatory statements, and seem reasonable and fair decisions. Yet as for the question of name-label, there is no pattern, because jurisdiction has also been exercised where fairly passive websites has been involved. The court in *Barrett* [67] noted that the posting of messages to listservs and Usenet discussion groups technically differs from the maintenance of a "passive" webpage because messages are actively disseminated to those who participate in such groups. However, for jurisdictional purposes, the court found that these contacts were akin to a "passive" website and insufficient to trigger the court's jurisdiction.

In *Lofton v. Turbine Design, Inc*.[68] in rejecting both specific and general personal jurisdiction the court found defendant's website was passive and "solely [ ] an advertising tool". The site contained defamation in relation to disparaging comments about plaintiff, a competitor. The court noted that unlike *Calder* the forum state in the matter, Mississippi, was not the focal point nor necessarily the locale of the alleged harm suffered. The plaintiffs persuasively argued that the defendants purposefully directed the alleged defamatory material published on their website toward Mississippi residents and a Mississippi corporation intending to harm their business activities and reputations. However the court pointed out that in the instant case, there is no evidence of any contact at all between the defendants and the forum state, absent the Internet and to find the existence of personal jurisdiction of a non-resident defendant based solely upon the postings on his website, which is simply accessible by Mississippi residents, is not the application of the law within this [fifth] circuit.

Otherwise, in *Telco Communications v. An Apple A Day*[69] - granting jurisdiction and the allegedly improper behavior transpired on the Internet – where the court found defendant was conducting business over the Internet, because defendant was advertising the firm and soliciting investment banking assistance in posting the press releases and that two or three press releases arose to the level of regularly doing or soliciting business. The court noted

[67] *Barrett supra* note 26, at 728.
[68] *Lofton v. Turbine Design, Inc*., 100 F.Supp.2d 404, 411 (N.D.Miss. 2000).
[69] *Telco Communications v. An Apple A Day*, 977 F.Supp. 404, 406-407 (E.D.Va. 1997).

defendant's use of a computer instead of paper did not distinguish defendant from cases where a defendant sends allegedly defamatory letters written to people throughout the country, including the forum state.

If the pattern from *Zippo* is to be followed, it has to be added that the court also pointed out approximately two percent of defendant's subscribers were forum residents. Thus, the Zippo court for naming a website "clearly doing business" requires that a certain amount of the sales is done with the forum and not just a few fortuitous.

In *Hockerson-Halberstadt* the court[70] labeled the website as doing e-commerce, but rejected exercise of jurisdiction because even though the sales to the forum over the last 18 months was $32,252 it was less than 0.0000008 of defendant's total sales during that period. The Molnlycke court follows this line by labeling the website as "not central to defendants business." Otherwise, in *Bochan v. Harris*[71] where defendant sold computer on-line. This court labeled the website as interactive and exercised jurisdiction even though there was no evidence of the amount of sales to the forum.

The court in *Winfield*[72] labeled the website only as an isolated advertisement in a nationally distributed magazine. It rejected jurisdiction, even though the defendant conducted sales through the on-line auction house, eBay, whereas, the court in *Origin Instruments*[73] labeled the website as having a moderate level of interactivity, and rejected jurisdiction. Here the defendant sold software through a link to "BuyDirect.com."

In *Hurley*[74] the court, rejecting jurisdiction, labeled a website allowing customers to make hotel reservations, as having an interactive quality beyond a passive website, whereas, the court in *Decker*[75] classified a similar website as commercial, but nevertheless rejected to exercise jurisdiction.

A name-level system just does not work. Websites are either interactive or not. A clearly doing business site is eo ipso also interactive; and a passive

[70] *Hockerson-Halberstadt, Inc. v. Costco Wholesale Corp*., 2000 WL 726888 (E.D.La., 2000).
[71] *Bochan v. La Fontaine and Harris*, 68 F.Supp.2d 692 (E.D. Va. 1999).
[72] *Winfield Collection supra* note 17, at 749.
[73] *Origin Instruments supra* note 55.
[74] *Hurley v. Cancun Play Oasis International Hotels*, 1999 WL 718556 (E.D.Pa. 1999).
[75] *Decker v. Circus supra* note 36.

website should indicate that jurisdiction cannot be exercised.

If court wishes to use a (gliding) scale as suggested by *Zippo*, they have to strictly follow and accept that the only variable in the scale is the interactivity of the website. Furthermore, the zero-point, named by *Zippo* as "passive", is equal to inactivity and cannot (alone) support exercise of personal jurisdiction. However, the practical purpose of such a scale is somewhat elusive, since the jurisdictional question only can be solved by granting or rejecting a motion to dismiss for lack of jurisdiction, that is, only to be two groups: A) The Rejecting Group including "passive websites" and B) The Exercising Group ("The Sufficient Interactive Group"). Such a grouping is the only one supported by the Due Process Clause.

4.5. Cyberspace Jurisdiction

A reading through more than ten years of U.S. court decisions involving Cyberspace facts, and especially on the issue of personal jurisdiction, shows first of all that the U.S. courts have realized the importance of having technical knowledge of how Cyberspace and international networks function along with knowledge of their positive possibilities and possible setbacks.[76]
Secondly, most U.S. courts, in relation to cases involving Cyberspace facts, have carefully taken into consideration that something uploaded to the Internet is accessible for everyone with an Internet-connection. Therefore, a court's decision will have international implications; if the court does not narrow, its ruling and find facts that point particularly at the state where the

[76] Justice Souter wrote in his concurring opinion in *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727, 777 (U.S. (Col), 1996): "And as broadcast, cable, and the cybertechnology of the Internet and the World Wide Web approach the day of using a common receiver, we can hardly assume that standards for judging the regulation of one of them will not have immense, but now unknown and unknowable, effects on the others...[W]e know that changes in these regulated technologies will enormously alter the structure of regulation itself, we should be shy about saying the final word today about what will be accepted as reasonable tomorrow. In my own ignorance I have to accept the real possibility that "if we had to decide today ... just what the First Amendment should mean in cyberspace, ... we would get it fundamentally wrong."

court is placed.

Furthermore, the research on U.S. Cyberspace-cases shows that many U.S. attorneys representing non-residents in the last couple of years have raised the question of whether the court at issue was the proper court since the defendant's use of Cyberspace reached every nation.

Most of the U.S. courts seem to have worked out the requirement that Cyberspace facts must positively point at the forum state and facts of doing business with the forum state. For example, in *Euromarket Design*[77] there was no doubt that the defendant had made an on-line business with prices listed in U.S.-dollars. The court made its determination on more facts than only the website's business-contents. It noted that the non-U.S.-defendant sold U.S. related and U.S. made products.

It is also worth noticing that no U.S. courts yet have determined general personal jurisdiction on basis of pure Cyberspace facts,[78] implying defendant being present in the forum state for any type of case or claim. Some courts considering general personal jurisdiction in respect to Cyberspace involvement have required that the on-line business must be central for the defendant's entire business and there must be evidence of high amount of sales with the forum state.

This means, that the U.S. courts only have decided jurisdiction on the requirements for specific personal jurisdiction or what could be called an extraordinary jurisdiction rule.

The research also shows that a system of a three-grouping of websites is wrong and without any practical purpose, because the jurisdictional question can only be answered by exercising or rejecting. A division between passive and interactive (inclusive e-commerce) is without any interest as long as some courts exercise jurisdiction even though it classifies the activity of the website as passive.

When determining whether a non-residents website is basis for exercising personal jurisdiction, the U.S. courts first look at the nature or kind of the website.

[77] *Euromarket Design, Inc. v. Crate & Barrel Ltd*., 96 F.Supp.2d 824, 840 (N.D.Ill., 2000).

[78] See this book chapter 3 section 3.3.4.1.1 and HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION, Chapter 32 section 1.2 (DJØF Publishing, 2004 Copenhagen - ISBN 87-574-0890-1).

A non-commercial website will only be found supporting jurisdiction if the contents are defamatory, and the target-point is found to be in the court's forum state. The U.S. courts have had various interpretations of what the target-point is. In a broad sense, the same can be said about defamatory communication occurring through (public) international networks. Otherwise, the website will only be regarded as nothing more than an informational method or source, which is not sufficient to exercise personal jurisdiction. The court in *Jewish Defense Organization v. Superior Court* [79] pointed out that when a consumer logs onto a server in a foreign jurisdiction he is engaging in a fundamentally different type of contact than an entity that is using the Internet to sell or market products or services to residents of foreign jurisdictions.

If the website is commercial in nature, the court will look thoroughly at the interactivity of the website. The trend seems to be that only if the website allows on-line business with payment, will U.S. courts hold that the non-resident was doing business through the website. Exercise of (specific) personal jurisdiction will only be granted if there is evidence that the defendant actually has done business with forum residents. Otherwise, the courts will regard the existence of the defendant's website as one of many circumstances that all together might support personal jurisdiction. Here, the courts have many different points of views, as the possibilities of interactivity of a website are as diverse as the human mind.

In the U.S. cases where Cyberspace has been involved, only a small percentage of the cases can truly be classified as Pure On-Line cases, and thus represent the specific problems that Cyberspace has created.

The reality in most cases is that there is also evidence of facts not related to Cyberspace. Therefore, Cyberspace facts have only been a part of all the facts in the minimum contacts test.

The real new aspect is found in the cases where the courts have exercised jurisdiction on Cyberspace facts alone and where one of the parties is an alien. In these relatively rare cases, the courts seem to have determined the exercise of personal jurisdiction on basis of a highly political view.

[79] *Jewish Defense Organization, Inc. v. The Superior Court of Los Angeles County*, 72 Cal.App.4th 1045 (Cal.App. 2 Dist., 1999).

Some courts do not want to bully the rest of the world with the legislation of the court's forum. They are reluctant to take a case into court, and thus respect the right for the users outside the courts forum and nation to be able to continue using the disputed Cyberspace facility. These courts use the second prong in the Due Process Clause - fairness and substantial justice - to "get rid" of Cyberspace cases. Thus, allowing the International dimension of Due Process being the determining factor. A "way-out" that is not available for many other nations court.

Nevertheless, the research on the U.S. Cyberspace cases does show that even having the genius and brilliance of the U.S. personal jurisdiction system built over a few words in the 14th Amendment with a discretionary second prong – the fairness and substantial justice – and the flexibility in the Due Process' "minimum contacts test", courts in the U.S. have still had tremendous problems adjusting the previous patterns to the world wide networks as Cyberspace being everywhere.

This can only imply even greater problems for the courts outside the U.S., which usually have very rigid jurisdictional rules over non-residents.

In *Reno-4,* the Third Circuit quoted the U.S. Supreme Court stating that "People in different States vary in their tastes and attitudes and this diversity is not to be strangled by the absolutism of imposed uniformity."[80]

The U.S. Supreme Court has more than once emphasized that the Internet is a international system and rejected in *Reno-2* to apply a "community standards" criterion to the Internet, because it would mean "that any communication available to a nation-wide audience [would] be judged by the standards of the community most likely to be offended by the message."[81] Nevertheless, a few states' governments have tried to bully its community standards to the Internet reaching far beyond their borders. This is especially the case where the contents violate a state's consumer protections laws. An example of this is the Minnesota Attorney General making a website with the headline, "Warning to all Internet users and providers…Persons outside of Minnesota who transmit information via the Internet knowing that information will

[80] *ACLU v. Reno*, 217 F.3d 162, 178 (3rd Cir. 2000) *quoting Miller v. State of Californi*a, 413 U.S. 15, 33 (U.S. (Cal), 1973).

[81] *ACLU v. Reno*, 217 F.3d at 167 and U.S. Supreme Court in *Reno v. ACLU*, 521 U.S. at 877-878.

be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violation of state criminal and civil laws…Whether a company solicits using the telephone, the mails, television or the Internet, the rules against fraud and illegal conduct are the same…There is no "Internet Exception" in our consumer protection laws."[82]

It should be inappropriate for any fortuitous court worldwide to decide jurisdiction on only the contents – call it advertising - of a website, and try to police the web totally selfishly only regarding its own consumer protection and not the rest of the worlds.

The research of the cases in the federal republic of fifty fairly independent states in United States of America imply that it is urgent for the entire world before chaos happens, that the world's courts and governments realize that Cyberspace and Internet can only work if every nation and every citizen respects that no rule can, in fairness, be applied if it will influence Cyberspace or Internet. It requires thoroughly thinking and shrinking the rules so they will not have an impact on the users of Cyberspace and Internet outside their own territory.

In International Law and Law of Treaties with respect to jurisdiction-rules, the connection-issue is vital. Further vital is the foreseeability in respect to which countries a foreign defendant can inspect to be call into court. The U.S. Constitution's Due Process Clause in the 14th Amendment can be regarded as an international jurisdictions rule similar to the Brussels Regulation, but opposite EU's rules, the Due Process clause is global, because it covers all foreigners that are being call into any state in the U.S. The Supreme Court of the U.S. has chosen not to censor/rewrite any of the states long arm statutes but in stead set out an upper limit, when a foreigner can be called into an American court. The Court has done it by drawing up a two part test, that is familiar with international law, that require a connection has to be actual and foreseeability ("minimum contacts test") and further take "fair play and substantial justice" into consideration.

The international society in the "brick and mortar" world, as in Cyberspace, will only accept and follow rule-making if it is internationally based,

[82] <www.ag.state.mn.U.S./home/consumer/consumernews/OnlineScams/ggpress.html> (visited March 15, 1999).

which reject every single areas rule (outside that special single area). Without international rules on enforcement, a court's decision over a non-resident will be without effect.

4.6. Conclusion

We live in an age when technology pushes us quickly ahead, and the law struggles to keep up. A number of existing statutes and common law precepts seem to serve surprisingly well in this dramatic new environment the Internet.[83]

The Zippo case is still the leading case if the decision is used faithfully. When one views the tables above – build on basis of several hundred cases and further tables[84] – the pattern is pretty clear. In cases where the courts have thoroughly examined the content of the website and its activity nearly all courts have only exercised specific jurisdiction over a commercial website if it allows both online sale and payment, and there is evidence of sales to the forum state. Thus, the examination of websites interactivity is vital and only if the point on the activity-scale is very high will the overwhelming amount of courts in the U.S. holds exercise specific jurisdiction based on a website.

Some courts even require a substantial amount of sales to the forum, because these courts regard a few sales not reaching the requirement of purposeful target the forum state. This pattern complies with rules in international law that a state is not allowed to call a non-resident into a country's court without evidence of foreseeability and fair play.

As for the question of personal jurisdiction and Cyberspace the lesson learned from the United States should at least be that the final test for any court worldwide before calling a non-resident using the international borderless "territory" of Cyberspace to its courtroom must be a determination of whether exercise of jurisdiction is consistent with fair play and substantial

[83] *Flesher v. University of Evansville* (Supreme Court of Indiana, No. 82S04-0008-CV-477, October 2001) <http://www.state.in.us/judiciary/opinions/archive/1001001.rts.htm> (visited December 2002).

[84] SPANG-HANSSEN-1 *supra* note 1, at 322-333.

justice. Otherwise, no court can later expect enforcement of its decision over a non-resident in another nation.

CHAPTER 5

Online Newspapers

A "pure online" example

By Henrik Spang-Hanssen[1]

5.1 Introduction

Online newspaper is a good example of "pure online" incidents that have created new issues to which previous law does not fit. In many incidents the "newspaper" is not based on subscription but rather just offering free information as everything else on the Internet. Thus, it does not have to have any (special) connection with the reader, and might achieve its revenue – if any - from advertising related to other parts of the world than that of the reader. The following shows that much news-information is given without fees, but some courts try to impose a "geographical zoning online that mirrors geographical offline."[2]

The Internet has created a new media for authors, journalists and publishers. In some instances is popular concern over the legal questions of Cyber-

[1] I'll like to thank Professor Kerry MacIntosh, High Tech Law Institute for comments to this chapter.

[2] Lisa Guernsey, *Welcome to the Web. Passport, Please*?, THE NEW YORK TIMES – TECHNOLOGY, March 15, 2001, <http://tech2.nytimes.com/mem/technology/techreview.html?res=9B01E7D71F3AF936A25750C0A9679C8B63> (visited November 27, 2005).

space actually no "new" issue worth discussing[3], but on the other hand in some circumstances of Cyberspace does it indeed give rise to new legal questions.[4] On the positive site, the Internet has created a low cost media that allows publishing at the same time to the whole world in one quick and easy step.

On the other hand, it has created new problems for authors, journalists and publishers as they - opposite the situation in the brick and mortar world – now can expect their writings to become available everywhere and to everyone unless they do something that hinder some people access to their published material.[5] If they do not hinder access they can expect liability claims from persons around the whole world that might have been hurt, because the reader comes from a different culture, religions etc. Thus, the writer's free speech rights in his own nation might not protect him, if the reader is outside the writers or publishers nation and that nation's legislation support remedies or criminal prosecution.

Further, as the writing being uploaded to the Internet is available in any nation – except where access has positively been hindered by the publisher –

[3] I. Trotter Hardy, *The proper Legal Regime for "Cyberspace"*, 55 U.Pitt.L.Rev. 993, 995 (1994).

[4] *Information Notice of 1. November 2002, E-Policy and E-Regulatory Framework Development in Transition Economies*, U.N. Economic Commission for Europe, para 4 at <http://www.unece.org/etrades/ict/docs/infonotice.pdf> (visited November 2003). "It should be observed that the Internet has become the modern equivalent of a telephone or a daily newspaper, providing a combination of communication and information that most employees use as frequently in their personal lives as for their work." The city agencies allowed workers to make personal calls if it did not interfere with their work performance, *Department of Education v. Toquir Choudhri* (Administrative Law Judge John Spooner, New York City Office of Administrative Trials and Hearings, March 6, 2006 – OATH Index no. 722/06), at <http://files.findlaw.com/news.findlaw.com/hdocs/docs/nyc/doechoudri30906opn.pdf#search='toquir%20choudhri'> or <http://search.citylaw.org/OATH/06_Cases/06-722.pdf#search='toquir%20choudhri'> (visited May 3, 2006) .

[5] The application of the principles of *Keeton v. Hustler Magazine, Inc*., 465 U.S. 770 (U.S. 1984) to Internet cases requires refinement. For while magazine publishers can affirmatively decide not to sell or distribute magazines in certain forums, this option of bypassing particular regions is not yet available to Website providers, *Hasbro, Inc. v. Clue Computing, Inc*., 994 F.Supp 34, 42 (D.Mass. 1997).

the author, journalist and/or the publisher has the risk of being sued at the same time in all the nations in the world for the same expression/writing. In the brick and mortal world, a person publishing something would only be at one location, which might allow a very high degree of free speech, for example "published" at Speakers' Corner in Hyde Park in London.[6]

The first fully web-based newspaper began in 1990 as a singe PC-based online product at Albuquerque Tribune. Another fully web-based newspaper, The Palo Alto Weekly began in California early 1995.[7] The number of online newspapers raised from 20 in 1994 to 1,600[8]-2,700 in 1999.[9] Of these total, about 523 newspapers covered general news on a timely fashion.[10] The New York Times started its online Web edition in early 1996.[11] Virtually all major U.S. newspapers now offer some form of online product.[12]

The Wall Street Journal has accumulated more than 500,000 paid sub-

[6] The Landgericht Hamburg ruled on 5 December 2005 that German newspaper Heise Online was immediately liable for reader comments and ordered the online newspaper to prevent publishing reader comments by previewing all comments, see HEISE ONLINE NEWS of 6 December 2005 <http://www.heise.de/english/newsticker/news/67029>. This order was a follow up on the previous order in *Universal Boards GmbH & Co. KG. v. Heise Zeitschriften Verlag GmhH & Co. KG* (Landgericht Hamburg, 20. September 2005 (Zivilkammer 24) – Docket No. 324 O 721/05) at <http://www.buskeismus.de/urteile/324O72105_dolzer-vs-heise.pdf> (visited March 2006). This is contrary to the German Supreme Court [Bundesgerichtshof (BGH)] in Karlsruhe previous decision that providers can only be held liable if there were reasonable ways of reviewing the content.

[7] *David Carlson's online timetable*. David Carlon's Virtual World at <http://iml.jou.ufl.edu/carlson/1990s.shtml> (visited October 17 2004).

[8] H. Levins, *Time of Change and challenge (Online Newspapers)*, EDITOR & PUBLISHER, 130 (1) page 58.

[9] Chip Brown, *Fear.com The State of the American Newspaper*, AMERICAN JOURNALISM REVIEW, 21, June 1999, page 51-71. <http://www.ajr.org/Article.asp?id=3230> (visited October 17 2004).

[10] Eric Meyer, *More Get Caught Up in the Web*, AMERICAN JOURNALISM REVIEW, 6 February 2001, <http://newslink.org/emcol8.html> (visited October 17 2004).

[11] H. Levins, *Time of Change and challenge (Online Newspapers)*, EDITOR & PUBLISHER, 130 (1) page 58.

[12] Jack Lovelace & Kirk Hallahan, *Pricing, content and Identity Issues at U.S. Online Newspapers – A Survey of Editors*, August 2003, page 1, at <http://lamar.colostate.edu/~pr/onlinelovelace040103.doc> (visited October 9, 2004).

scribers, but has nevertheless had to reduce its staff at WSJ.com because of lacking surplus.[13]

The Internet ranks second only to television as a medium of choice for breaking and new information.[14]

> A survey of August 2002 showed nine out of the top 20 news websites in U.S. were affiliated with newspapers. Five of the top 20 news websites in U.S. were affiliated with TV-news channels. Only one of the top 20 news websites in U.S. seems to be a pure online newspaper-firm (drudgereport.com).[15]

5.2. Scope

It is my main view that when discussing the Cyberspace and international public computer network (including the Internet) one should only deal with issues that are special for this media and thus require special handling; whereas the Internet in all other regards should be treated as any other old media, thus using old legislation to solve a certain issue. The main task is thus to find the issues that are special for the international public computer network. The significant new thing about the Internet or international public computer networks is that what before had to be "transported" by use of tangible effects in the brick and mortal world now can be "transmitted" with electronic bits via computer network. Thus, the new issues belong to the italic

[13] *Id* at page 3, and Mark Jurkowitz, *Online News Outlets Catch Their Breath*, THE BOSTON GLOBE ONLINE, 19 January 2001, at <http://digitalmass.boston.com/news/daily/01/011901/online_media.html> (visited October 17 2004), Aparna Kumar, *Online News Frenzy Is Fizzling*, WIRED NEWS, 12 January, 12 2001 at <http://www.wired.com/news/business/0%2C1367%2C41121%2C00.html> (visited October 17 2004).

[14] Jack Lovelace *supra note* 12 at page 4.

[15] Carl Sullivan, *Papers Run Nearly Half Of Top 20 News Sites*, EDITOR & PUBLISHER, September 12, 2002 at <http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1698470> (visited October 7, 2004).

written fields in the following tables:[16]

Contents of Messages

	Sent by person in country A	**Sent by person in country B**
Received by person in country A	Law of country A	*Sending electronic mail: (New) Cyberspace jurisdiction & law*
Received by person in country B	Sending by normal mail: Normal International Postage's Law/ Acts between the countries	Law of country B

Information on Web-pages

	Made by person in country A	**Made by person in country B**
Read by person in country A	Law of country A	*(New) Cyberspace jurisdiction & law*
Read by person in country B	(New) Cyberspace jurisdiction & law	Law of country B

[16] HENRIK SPANG-HANSSEN: CYBERSPACE JURISDICTION IN THE U.S.: THE INTERNATIONAL DIMENSION OF DUE PROCESS, ISBN 82-7226-046-8, which also freely can be downloaded at <www.geocities.com/hssph> [hereinafter SPANG-HANSSEN-1].

Trade/commercial through Internet

	Vendor is person in country A	Vendor is person in country B
Buyer is Person in country A	Law of country A	*Delivered electronic/By downloading: (New) Cyberspace jurisdiction & law* [17]
Buyer is person in country B	Tangible things: (Delivered by carrier)[17] "Normal" jurisdiction "Normal" law (consumer / agreement)	Law of country B

Table 5.1: Where new law may be needed

In the following, it will be presumed that the issue is "*pure on-line*", that is, no physical shipment or tangible things are involved, and at least one user is a foreigner, which is a non-resident or non-national. Thus, the pre-condition is "pure online" cases, and this chapter will not deal with paper versions of newspapers delivered in the "brick and mortar" world. The term "*online newspapers*" will in the following be regarded as newspapers that have been delivered online and have passed national-borders, thus the receiver is out-of-state (matters inside a nation is not the issue).

The structure of the Internet as a new media for publication has given rise to new aspects such as Deep Linking,[18] Copyright[19], Advertising[20], Personal

[17] Dilemma: two kinds of rules when for example selling software:
If delivered pr. ordinary mail/post => normal law and normal jurisdiction
If delivered electronic/downloading => no law and no jurisdiction.

[18] Philip G. Hampton, *Legal Issues in Cyberspace*, 759 PLI/PAT 537, 602-614, Karren M. Shorofsky, *The Wide World of Websites: Other current Internet legal topics*, SD38 ALI-ABA 451 (1999); Henrik Spang-Hanssen, *Indtrængen ("deep linking") i andres databaser* [Deep linking in others databases] LOV & DATA page 1-3, [Law and Data Journal] 4/2001] (Published in Scandinavia, ISSN 0800-7853). *See* also *Home A/S v. OFIR a-s* (The Maritime and Commercial Court in Copenhagen, 24 February 2006 - docket No. V-108-99), <http://www.domstol.dk/media/-300011/files/v010899.pdf>, below in chapter 8 section 8.4.2.

[19] *Los Angeles Time v. Free Republic*, 1999 WL 33644483 (C.D.Cal. Nov. 8, 1999 – CV 98-7840-MMM)(Members of a "bulletin board" website copied newspaper articles

Jurisdiction with only bits-contact,[21] Taxation, E-money, Electronic agents,[22] Pornography[23], issues this article will not deal with.

This chapter will briefly mention issues of the U.S. Commerce Clause and zoning in section 5.3. It will deal with the issue of online newspapers that are available outside the nation where the publisher is located. Section 5.4 will briefly mention some rules on free speech related to publication. In overall, this chapter will deal with the question of online newspapers liability risk in relation to defamation-rules in section 5.5-5.7. The chapter ends with Final Remarks, section 5.8.

5.3. Rules on Cross-Border

Online newspapers have at least two special issues that are not an issue for paper-version newspapers. One is the question of where the newspaper is read – or where and which are its customers; the other question is by what rules the newspaper has to be issued.

and posted them on the "bulletin board" website with their remarks or comments). Court enforced newspaper's copyright and held it did not restrict the "bulletin board['s]" free speech rights). See also, 17 U.S.C.A. §512 on limitations on liability relating to material online and Copyright infringement.

[20] Karren M. Shorofsky, *Advertising and Promotions on the Internet*, 563 PLI/PAT 659.

[21] A survey of US cases from 1991-2000 showed that in only 1.5 % of published cases related to Cyberspace were the personal jurisdictional question decided on Cyberspace facts alone, see SPANG-HANSSEN-1 *supra* note 16, at 138..

[22] Emily M.Weitzenböck, *Electronic Agents and the Formation of Contracts, International* JOURNAL OF LAW AND INFORMATION TECHNOLOGY, VOL. 9 NO. 3, 204-234, (Oxford University Press 2001) <http://www3.oup.co.uk/inttec> (visited July 2003) and Emily M.Weitzenböck, *Good Faith and Fair Dealing in Contracts Formed and Performed by Electronic Agents*, *in Chapter 9 of* YULEX 2005 (Institutt for rettsinformatik, Oslo University 2005 – ISBN 82-7226-094-8).

[23] A Danish newspaper "Ekstrabladet" – which has an online version - contains in every issue "the Page-seven girl" that probably would offend people in many foreign countries, but is legal under Danish Press rules and thus daily makes the newspaper a potential defendant in several countries in the world, including California, which has a large tax-income from export of porn-movies.

5.3.1. What law has to be followed?

As for the latter question, initially should be pointed out that historically newspapers were issued in the town were its customers were. Later newspapers became regional or national. However, this did not change the legal scheme for the newspaper as it was still doing business inside an area that was covered with the same legislation and thus the same rules for the newspaper. Some newspapers have chosen to sell also abroad, but in its choice of new markets it still has had the full discretion to choose where it wanted to sell and thus under what laws.

When publishing on the Internet the newspaper suddenly become worldwide – or rather being at the place of its fortuitous readers – and thus does not have the ability to choose its market – many online newspapers does not require real (payment) subscription.

Thus, the question rises, which nation(s) can determine under what rules the newspaper is issued. This question is decided not by that nation but by the international society of nations.

International public law on jurisdiction to prescribe in relation to international computer network can be summoned up as in the below table as for Pure Online cross-border & the Nationality[24] and Territorial[25] Principles. It should be added to the table that the Subjective Territoriality Principle[26] allows State D to prescribe in all of the fields, whereas the Active Personality Principle[27] allows the State of nationality or residency of the suspect to prescribe in all of the fields.[28]

[24] The Nationality principle confers jurisdiction over nationals of the State concerned. It can be divided into the Active Personality Principle & the Passive Personality Principle.

[25] The Territoriality Principle confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place. It can be divided into the Subjective Territoriality Principle & the Objective Territoriality Principle

[26] The Subjective Territoriality Principle permits a State to deal with acts that originated within its territory, but was completed or consummated abroad.

[27] The Active Personality Principle is based on the nationality of the suspect. Public international law accepts jurisdiction over a state's owns citizens based on nationally, or the links between the individual and the state.

[28] See further HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION - POSSIBILITIES OF DIVIDING CYBERSPACE INTO JURISDICTIONS WITH HELP OF FIL-

	Made online from State D by national of state A	**Made online from State D by national of State C, but citizen of A**	**Made online from State D by national of State B**
Uploaded in State E	International Law involved State E regarded as sender or receiver state?	International Law involved State E regarded as sender or receiver state?	International Law involved State E regarded as sender or receiver state?
Received in State B	International Law involved Objective[29] and Passive[30] personality (controversial) principles allow State B to prescribe?	International Law involved Objective and Passive personality (controversial) principles allow State B to prescribe?	International Law involved

Table 5.2: Public International Law Principles Involved

This implies for online newspapers that it has to meet the requirements of the legislation in:[31]

- The State from where the original electronic communication ("bits-transfer") was prepared
- The State where the communication is uploaded
- The State of the newspaper's "nationality," that is, for a private owned newspaper where the owner is born, or a corporate is incorporated

TERS AND FIREWALL SOFTWARE page 300 (DJØF Publishing, Copenhagen, February 2004 - ISBN 87-574-0890-1) [hereinafter SPANG-HANSSEN-2].

[29] The Objective Territoriality Principle permits a State to deal with acts which originated abroad but which, at least in part, were (i) consummated or completed within their territory – the "Effect Doctrine"; or (ii) producing gravely harmful consequences to the social or economic order inside their territory - the "Protective Theory".

[30] The Passive personality principle or passive nationality principle - based on nationality of the victim, not the nationality of the offender.

[31] SPANG-HANSSEN-2, *supra* note 28, at 345.

- The State where the newspaper is a "citizen," that is, for a private owned newspaper where the owner living or a corporate is having headquarter

From the receiver site's perspective,[32] it should initially be noted that as the Passive personality principle generally is rejected by the international society, the newspaper out of this principle does not have to follow the legislation (statutes or case law) in the state of which the receiver is a nationality. However, the online newspaper might have to meet the requirement pursuant to the Objective territoriality principle that permits a State to deal with acts which originated abroad but which, at least in part, were

- consummated or completed within their territory (the "effect doctrine"); or
- producing gravely harmful consequences to the social or economic order inside their territory (the protective theory).[33]

As for jurisdiction to adjudicate, courts seem to take cases on basis of national rather than international rules, see for example French court over Californian Yahoo,[34] American court over Canadian iCraveTV (mentioned further below).[35] Another issue is enforcement, that is, whether one nation's court decisions will be allowed enforced by the courts of a foreign nation whereto the decision is sent for enforcement.

In respect to legislative and enforceable issues, it should be noted that certain groups' of nations have made rules, which forbids a nation to make legislation contrary to the groups declared principal interest of interstate commerce. This is the case between the Member States in the European Union[36]

[32] *Id.* 346.

[33] The protective theory covers a variety of political offences and is not necessarily confined to political acts. The principle is well established and seems justifiable because it protect a state's vital interests. However, it can easily be abused. The decisive is the importance of the offence, which standard is supplied solely by international law.

[34] SPANG-HANSSEN-2, *supra* note 28, at 184-189, 463-466, 483-517.

[35] *Id.* 478-482.

[36] See articles 25, 28 & 81 of the E.C. Treaty: "The following shall be prohibited as incompatible with the common marked: all agreements between undertakings…which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the common market". *EU Commission v. Kingdom of Spain* (E.C.J. C-358/01 of 6 November 2003) (Violated EC

and the United States of America. To a certain extent participants of the WTO are hindered from making legislation that is contravening to the common commerce denominator.

As for free speech and international public law, there exists no international law stating a nation's citizen has to cut off content that is legal in at least one foreign nation besides the citizens own nation - and thus probably acceptable to the U.N. Declaration of Human Rights on free speech. However, there does exists a treaty concerning suppression of the circulation of obscene publications (writings, drawings, pictures or articles), which also fits electronic transmission.[37]

5.3.1.2. United States

As for the United States, its Constitution Article I, Section 8, Clause 3, the so-called Commerce Clause, states: The Congress shall have Power…To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes.

The U.S. Supreme Court has elaborated the negative to this clause in the "Dormant Commerce Clause": Even where Congress chooses not to exercise such power, States cannot regulate, even if Congress "sleeps."38 However, when Congress acts in a way that grants states permission to burden interstate commerce, the courts may not interfere - a "reconveyance" of federal author-

art. 28) & *Tribunale di Ascoli Piceno v. Gambelli*, (E.C.J. C-243/01 of 6 November 2003) (Italian prohibition violated (EC art. 43 & 49). The EU Directive on electronic commerce "removes obstacles to cross-border online services in the Internal Market and provides certainty to business and citizens alike," page 3 of FIRST REPORT ON THE APPLICATION OF DIRECTIVE 2000/31/EC, EU COMMISSION, COM(2003) 702 FINAL OF 21. NOVEMBER 2003 at < http://europa.eu.ont/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf>.

[37] Treaty of 4 May 1910 as well as protocol of 4 May 1949, Nuveau Recuceil de Traites/G.Fr. de Marters, 3 serie, VII, 1913 p. 266-272, UNTS 30 (1949) p. 3-22 and UNTS 47 (1950) p 159).

[38] The Supreme Court has developed two methods of dealing with constitutional challenges to state regulations in *Pike v. Bruce Church, Inc*., 397 U.S. 137, 142 (U.S. 1970) (initiating a balancing test) and *Oregon Waste Systems, Inc. v. Department of Environmental Quality of The State of Oregon*, 511 U.S. 93, 100-101 (U.S. 1994).

ity.[39] The doctrine consists of four principles:[40]

- laws that directly regulate commerce occurring in other states are invalid,
- laws that amount to "mere economic protectionism" are also invalid,
- laws that discriminate on their face are rarely upheld and must be shown to advance a legitimate local purpose that cannot be adequately served by reasonable nondiscriminatory alternatives, and
- when a statute has only indirect effects on interstate commerce and regulates evenhandedly, courts examine whether the State's interest is legitimate and whether the burden on interstate commerce clearly exceeds the local benefits.

In Dormant Commerce Clause jurisprudence, the least-restrictive-means test asks whether the state regulation "could be promoted as well with a lesser impact on interstate activities."[41]

Thus, interstate commerce is controlled by the applicable acts of Congress governing the rights of the parties to such transactions, and the Dormant Commerce Clause prohibits states from exporting their laws into the local markets of sister states. This implies, that "although one engaged in manufacturing or processing may be regarded as not engaged in interstate commerce, when the goods are intended to be transported in interstate or foreign commerce, stoppage for manufacture or compression does not give any part of the transportation an intrastate character. Upon a like principle, the transportation or transmission of electric current direct from the seller in one state to the consumer in another for immediate or practically immediate use, subject only to a temporary stop en route for the purpose of reducing the current to a commercial voltage, remains interstate commerce until the commodity has

[39] *Merrion v. Jicarilla Apache Tribe*, 455 U.S. 130, 154-55 (US 1982), *Fulton v. Faulkner*, 516 US 325 (U.S. 1996) (opinion on method of dormant Commerce Clause analysis).

[40] *Bainbridge v. Turner*, 311 F.3d 1104, 1112 (11th Cir. 2002)(out-of state wine-sales & 21st Amendment)

[41] Jack L. Goldsmith, *The Internet and the Dormant Commerce Clause*, 100 YALE L.J. 785, 817 (March 2001); H. Joseph Hameline & William Miles, *The Dormant Commerce Clause Meets the Internet*, 41-OCT B.B.J. 8 (1997).

reached its goal."[42]

Similarly, for newspapers this indicates that a state should not be allowed to regulate newspapers that might be stored on a proxy-server (temporary stop) placed in that state. However, at least some states outside the U.S. have held this to be sufficient for exercising jurisdiction (and thus legislate). Generally, Internet regulation runs afoul of the Dormant Commerce Clause because the Clause "protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State."[43] Thus, at the same time that the Internet's geographic reach increases a forum State's interest in regulating out-of-state conduct, it makes state regulation of the Internet impracticable.[44]

As for the content of online publishing, several state laws that have tried to "censor" this content have been regarded as violating the Commerce Clause, because the laws tried to regulate cross-border computer networks, for example a statute criminalizing computer materials harmful to minors hindered Internet information on women's health and interests, literary works and fine art, gay and lesbian issues, prison rapes, and censorship and civil liberties issues,[45] or a statute making it a crime to sell, lend, distribute or give away pornographic material, which was harmful to minors.[46]

The content of online newspapers is in the United States regulated by several rules. The main rule is the First Amendment of the U.S. Constitution – on this below in section 5.4.1.1. Others are the Single Publication Rule that is used in most states pursuant to either statute or case law, and in some states a

[42] 15A Am.Jur.2d Commerce §§ 7, 35 and 78 [American Jurisprudence on Commerce, 2nd Ed West Publishing] citing *Mills Creek Coal & Coke Co, v. Public Service Com*., 84 W.Va. 662, 100 S.E. 557, 7 A.L.R. 1081 (W.Va. 1919).

[43] *Healy v. Beer Institute*, 491 U.S. 324, 337 (U.S. 1989) (rejected out-of-state wine-sale & 21st Amendment).

[44] *American Booksellers Foundation v. Dean*, 342 F.3d 96, 104 (2nd Cir. Aug. 2003).

[45] *American Civil Liberties Union v. Johnson*, 194 F.3d 1149 (10th Cir. 1999). Also, *Cyberspace Communications, Inc. v. Engler*, 55 F.Supp.2d 737 (E.D. Mich. 1999) affirmed by 238 F.3d 420 (6th Cir. 2000) (criminalizing distribute sexually explicit materials to minors through computers); *American Libraries Association v. Pataki*, 969 F.Supp. 160, 169 (S.D.N.Y. 1997) (crime to use a computer to disseminate obscene material to minors).

[46] *American Booksellers supra* note 44, at 104.

Retraction statute – on this below in section5.5.

Furthermore, some online newspapers to a certain extent can partly function as bulletin boards where subscribers/readers can directly publish their point of views and comments, whereas a paper version always will require a person at the newspaper to process – and thus read - the reader's view before it can become available in the printed version. This as for online newspapers raise the question of whether the online newspaper partly should be regarded as an access provider and thus be covered by a Federal statute that immunize such providers – on this below in section 5.7.

5.3.1.2. Outside the U.S.

American online newspapers have by using international public computer networks to consider non-U.S. legislation, unless they hinder access to their newspaper for every person not physical in the U.S., where U.S. law surely will be the ruling one.

A worldwide survey of fall 2003 indicated that the gross revenue from outside the country of the media firm's office was between 1-10% for one-fifth of the answering media firms and between 11-25% for 17% of the answering media-firms.[47] Thus, firms are also relying on business abroad.

U.S. firms should especially be aware of the fact that outside the U.S. free speech is not interpretated as broadly as in the U.S., thus some content allowed in the U.S. might be illegal in foreign countries. Further, in most nations there exists neither a Single Publication Rule nor a Retraction statute, which makes questions of liability for the online newspaper much more essential than for paper versions.

> From raw-data of the world wide survey done in fall 2003 can be produced the following for the media-environment:[48]
> 59 % of the answers for media firms stated jurisdiction and applicable law concerns had become a more important issue for business since 2001. 59% of the answering firms had business on Internet/e-commerce and 28 % of an-

[47] ABA Cyberspace Committee/ICC world-wide survey of Fall 2003 indicated as for Media-segment (29 answers) – Computerized by Henrik Spang-Hanssen on 9 October 2004 from the survey-database – of which committee he was a member.

[48] *Id*.

swering firms had had incidents. The main concerns were consumer-protection laws (59%), e-commerce regulation (55%), taxation (35 %), defamation and other torts (31%) and privacy (28%). For 48% of answering firms was the primary concern focused on international jurisdiction or execution issues. 52% of the firms had adjusted the way it did business in response to jurisdictional concerns.
Of answering content provider-firms 28 % had altered is content in response to jurisdictional concerns.
73% of media-firms had terms of use agreements. Hereof 10% had an ADR clause. 25% held online business had become harder from a legal perspective since 2001 and 49% expected it be become harder by the end of 2005.

5.3.2. Where is the Newspaper published?

The above section indicates that as for what law governs, it is vital for online newspapers to know where their customers/readers are located in the brick and mortar world. In addition, as much of newspaper's revenue comes from advertising it is from a business perspective vital to know where their customers/reader is located.

In the brick and mortar world, a newspaper can pretty easy manage where its customers/readers are located, as the newspaper will have to physically ship the paper to the address of the reader, either by direct mail or through sales-booths. Thus, the newspaper has up front the choice of whether it wants to deliver to the reader's location – and thus have to obey that locations law.

Otherwise for the online newspaper that need technical skills to sort out potential customers/readers as the initially situation is, that anything uploaded to international public networks are available to everybody on the Earth with access to a computer with a modem. The Internet "enables inter-communication using multiple data-formats…among an unprecedented number of people using an unprecedented number of devices and among people and devices without geographic limitations."[49]

[49] Stated by expert witness in *Dow Jones v. Gutnick*, [2002] HCA 56 para 14, 42 I.L.M. 41, 2002 WL 31743880, 210 CLR 575, 194 ALR 433, 77 ALJR 255, [2003] AIPC 91-842, (High Court of Australia, 10 December 2002 - No. M3/2002).

From the ABA/ICC survey:50
94% of answering media-firms considered their website a significant element of its marketing strategy. Hereof 66% had global websites, of which 49% had country-specific websites. 59% was actively soliciting business via the website.
21% of answering media-firms had made efforts via the website to influence possible jurisdictional outcomes. The most used features were: language, currency, legal terms, local contacts points, local server and country-specific/consumer-specific content.
59% traced users' location – hereof 28% by user registration, 17% by user self-identification, 14% by billing address and 10% by geo-identification technology.
17% of media-firms blocked access from certain jurisdictions (10% Middle East/North Africa, 10% Europe, 31% Sub-Sahara Africa).

Besides the opportunity for the online newspaper to hinder access to the newspaper without a password issued by the newspaper – and thus give the newspaper beforehand an opportunity to choose what customers it wants (access to a newspapers private network) – the online newspaper can choose to use filtering out certain groups of cybernauts (public network). The preferred feature for this seems from the ABA/ICC-survey as for media-firms to be use of self-identification and geo-identification technology.

5.3.2.1. Geo-tracking

However, as for the latter, which allows newspapers to locate customers invisibly from the receiver's perspective, the more precise the software gives a location, the more unavoidable it is to intrude and violate privacy laws. Furthermore, geo-location tracking software[51] often bases its determination on the IP-address, but there is no inherent connection between an IP address

[50] ABA Cyberspace Committee/ICC world-wide survey of Fall 2003 indicated as for Media-segment (29 answers) – Computerized by Henrik Spang-Hanssen on 9 October 2004 from the survey-database – of which committee he was a member.

[51] Many names or terms have been given to this software, for example GeoIP, IP-location, Geo-computing, and User-location. See also Teemu Ross et al., *A Probabilistic Approach to WLAN User Location Estimation*, INTERNATIONAL JOURNAL OF WIRELESS INFORMATION NETWORKS, p. 155, Vol. 9, no. 3, July 2002, also at <www.cs.helsinki.fi/u/ttonteri/pub/ijwin02.pdf> (visited March 2006).

and its physical location.[52]

In general, the software is put into the newspaper's website. When an potential buyer access the website the seller's software will with help of algorithms check the location of the potential buyer or more correctly his computers IP address,[53] which is compared with the seller's software-company's constantly updated IP-database.[54] However, geographical identification tech-

[52] SPANG-HANSSEN-2, *supra* note 28, at 333-339. Otherwise, Dan Svantesson, *Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 111 (Fall 2004), who thinks present geo-location software is sufficiently accurate for legal purposes, even though he points out that" the accuracy of these products is difficult to gauge." However, for example *Ecommerce Taxation and the Limitations of Geolocation Tools* pages 3-5 & 7, Information Technology Association of America (ITAA) acknowledge that geolocation software only can check the geographic location of the point where the user's computer signal enters the Internet (the customer "joins the Internet"), but not the location of the user and only within 50 miles under the very best of circumstances. The examination paper notices that larger IP-address-users under IPv4 may only have a single bloc of IP addresses for the whole world. It further points out, that delays in reflecting changes in reassignments or incorrect changes to router tables, both will negatively impact the overall quality of the correctness of a geographic location. Another problem is that if a customer is not accessing a POP from the same geographic area as the POP server itself – which the geolocation technologies assume – then the geolocation software will send back inaccurate customer location data. Of this reason does wireless Internet access present unique problems. If a customer chooses to connect into an ISP outside of their local telephone calling area, their location will not be correctly reported by the geolocation software, for example where a user calls an ISP via a POP call-in number located in another state or country. In addition, the future IPv6 protocol that will have far more IP addresses and thus imply far more (dynamic) reassignment of IP addresses will probably overwhelm geolocation software capacities, at <www.itaa.org/taxfinance/docs/geolocationpaper.pdf> (visited March 2006).

[53] There's no reliable method to do the trick. However, certain methods of "detective work" can be found in for example Uri Raz, *How do I find the geographical location of a host*, given its IP address?, at <http://www. private.org.il/IP2geo.html> (visited June 2003).

[54] InfoSplit claims to determine the country of origin with 98,5 %, but this percentage "is misleading." For example many French people uses access-providers in Swiss and Belgium pursuant to Jean-Denis Gorin, Yahoo! Inc. expert witness and referred to at page 43 in French Court's RAPPORT DE CONSULTATION at <http://www.law-links.ch/archiv00.html file rapportyahoo-6nov00.zip> (visited May 2003).

nologies can be defeated by different software like anonymizers,[55] remote sessions via Telnet, and remote dial-up connections.[56] Furthermore, if a reader uses a Satellite Internet access provider it is difficult even to ascertain the country that the end user originates from.[57]

Further, the identification does not reveal whether it was the on-the-road in Arizona salesperson, English-speaking Mr. X, or Spanish-speaking Ms. Y in Nevada, or French-speaking Miss. Z that used the (same) laptop, which at night is stored at the reception of a company located in for example Silicon Valley, USA.[58] In the (international) law perspective, persons - not machines - are responsible for their work and dealings. The geo-locating tracking software does not work in (international) law because it is too insecure.[59] For advertising or marketing purposes, the accuracy is fine, but when it comes to the courts, a higher standard is needed.[60]

[55] See for example *What are the "A1" Anonymous Proxy entities* and *How do I tell what the IP address behind a proxy is?* MaxMind at <www.maxmind.com/app/faq>, <www.maxmind.com/app/proxy#open> (visited March 2006).

[56] See for example *Zero-Knowledge Systems' application "Websecure"* at <http://www.freedom.net/products/websecure/howitworks.html> and *Anonymizer's which effectively cloak IP addresses from mapping applications "PrivateSurfing"* at <http://www. anonymizer.com/privatesurfing> (visited 14 October 2003).

[57] Satellite providers serve high risk countries, see *What are the "A2" Satellite Provider enties?* MaxMind at <www.maxmind.com/app/faq> (visited March 2006).

[58] SPANG-HANSSEN-2, *supra* note 28, at 333-339; Michael Geist, *Is there a there there? Toward Greater Certainty for Internet jurisdiction*, 661 PLI/PAT 561, 612-615 (July 2001) or <http://aix1.uottawa.ca/~geist/ geistjurisdiction-us.pdf> (visited 2001) & Jack L. Goldsmith, *The Internet and the Dormant Commerce Clause*, 100 YALE L.J. 785, 810-816 (March 2001).

[59] *Ecommerce Taxation and the Limitations of Geolocation Tools* page 7, Information Technology Association of America (ITAA) concludes that geolocation technologies only has value where a high degree of accuracy regarding a user's jurisdiction is not required, at <www.itaa.org/taxfinance/docs/geolocationpaper.pdf> (visited March 2006) . See also *Benjamin Edelman, Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users* page11, at <http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf > (visited March 2006).

[60] SPANG-HANSSEN-2, *supra* note 28, at 333-339. Otherwise, *Dan Svantesson, Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Interne*t, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 117, 119 (Fall 2004), who

It is obvious that the determination of whether a newspaper has had a fair chance for determining, which law applies to a certain customer/reader, cannot be bases on a international nation-border-map made by a private software company and put on a newspapers website. The courts will without doubt reject an online newspaper arguing that the particular courts local laws do not bind it because the location-software had determined a customer/reader to be at another location than that of the court's resident in question.[61] Thus, an online newspaper in relation to its legal obligations should not rely on geo-tracking software to determine its customers.[62]

5.3.2.2. Customer self-identification

Another, feature used to locate customers/readers by the media-firms pursuant to the ABA/ICC survey is customer self-identification. However, this feature does neither seem to give an online newspaper the necessary assurance of the customer's location.

holds that "the courts must accept a rather high percentage of false positives when evaluating a Web site operator's use of geo-location technologies to exclude access by all but the access-seekers from a particular state, or group of states." He further notice, that there is persuasive reasons "to expect it to become harder, not easier, to produce accurate geographical analysis tools." As mentioned above in this book chapter 2, use of the new IPv6 protocol will not help geo-location software – presumably more make it less accurate.

[61] Former Bell Labs researcher Bill Cheswick, Lumeta Corp., to Stefanie Olsen, *Geographic tracking raises opportunities, fears*, CNET NEWS.COM, 8 November 2000, at <http://news.com.com/2100-1023_3-248274.html> (visited 14 October 2003).

[62] MaxMind's GeoIP has a failure-percentage of 12-55 depending on what country is in question. However, it claims their GeoIP databases are 99% accurate on a country level. As for City accuracy for different countries the percentage is from 45 % in United Kingdom and 57 % in Germany to 88 % in Belgium, see *GeoIP City Accuracy for Select Countries*, at <www.maxmind.com/app/city_accuracy>. Furthermore, it claims that it is 80 % accurate on a U.S. state level, and 75 % accurate for US cities, at <www.maxmind.com/app/faq> (visited March 2006). Detecting movement of a sensor in a network of communication nodes is a disturbed detection problem that has yet to be fully explored, Neal Patwari et al., *Locating the Nodes*, IEEE SIGNAL PROCESSING MAGAZINE page 66, no. 54, July 2005, also at <www-personal.engin.umich.edu/~npatwari/localizationMag.pdf> (visited March 2006).

The American court in iCraveTV[63] rejected to dismiss a case where Canadian defendant had limited its TV access to customers that had to identify themselves as living in Canada. The court found that a feature of self-identification gave cybernauts from outside Canada to easy an access to the Canadian media-website.[64] The website in question was meant solely for Canadian viewers that had to wade through several pages of legal language, log on by typing their Canadian area code, and click a button indicating that their computer physically was in Canada. [65]

Furthermore, it is a general rule that what technology can do is to pose barriers that are sufficient to keep those who are not strongly motivated from finding their way to inappropriate material or experiences. Once discovered, a method of circumvention is often proliferated widely.[66] Thus, an online newspaper has difficulty of effectively cutting of all the parts of cybernauts it does not want to deal with.

5.4. Free Speech Online

As online newspapers "can be" anywhere in the world it should be mentioned

[63] *Twentieth Century Fox v. iCraveTV*, 2000 US Dist Lexis 11670, 53 U.S.P.Q.2d (BNA) 1831 (W.D.Pa, Feb. 8, 2000). On the Internet-technical aspects of the case, see also Benjamin Edelman*, Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users* page 11, at <http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf> (visited March 2006).

[64] This will be an even bigger problem with cellular phone-TV. The Canadian Radio-television and Telecommunications Commission held in April 2006 that Mobile TV services from Bell Mobility Inc. and Rogers Wireless Communication Inc. are delivered over the Internet and not subject to the same rules as those provided by cable operators and broadcasters. Therefore, cell phone carriers should be able to experiment in the TV sector without immediately dealing with regulatory restrictions, Broadcasting Public Notice CRTC 2006-47 at <www.crtc.gc.ca/archive/Eng/Notices/2006/pb2006-47.htm> (visited April 2006).

[65] SPANG-HANSSEN-2 *supra note* 28, at 478-482,

[66] DICK THORNBURGH & HERBERT S. LIN, A GLOBAL INTERNET" IN YOUTH, PORNOGRAPHY, AND THE INTERNET section 11.2 (Dick Thornburgh & Herbert S. Lin, eds., National Academy Press, 2002), at <http://search.nap.edu/html/youth_internet> or <http://www.nap.edu>.

that there does exist an international statement of free speech in article 19 of the U.N. Declaration of Human Rights states: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[67] However, this declaration does not mean under international law that free speech cannot be limited by a nation through legislation.[68] Thus, under international law nations are to a certain degree allowed to make limits in people's right to publish their opinions, especially if it is related to national security issues, or culture and religious issues, which are often mentioned in a nation's constitution.

5.4.1. United States

As for news-information available inside the United States there exist at least one Constitutional amendment and one statute that has vital significance for online newspapers read by people inside the United States. These will in the following be mentioned very briefly.

> A recent case raised several novel and important issues affecting the rights of web publishers to resist discovery of unpublished material and the First Amendment status of Internet news sites – a case on whether online journalists were entitled to the same legal protections as their offline counterparts.[69] Apple Computer Inc. alleged that persons unknown caused the wrongful publication on the World Wide Web of Apple's secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers. Apple sought and obtained authority to issue civil subpoenas to the publishers of the Web sites where the information appeared. Much of the published information appeared to have originated in "an electronic presenta-

[67] UN Universal Declaration of Human Rights, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948.

[68] Confer Article 19(3) of UN International Covenant on Civil and Political Rights, Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966 - into force 23 March 1976.

[69] *Jason O'Grady v. Superior Court of Santa Clara County* (Apple Computer), 44 Cal.Rptr.3d 72, 2006 WL 1452685 at *6 (Cal.App. 6 Dist., May 26, 2006 - No. H028579), at <http://www.courtinfo.ca.gov/opinions/documents/H028579.PDF>.

tion file--or "slide stack,"" generated by Apple and "conspicuously marked as 'Apple Need-to-Know Confidential.'"" [70]

On February 14, 2005, petitioners moved for a protective order to prevent the discovery sought by Apple on the grounds that (1) their "sources and unpublished information" were "protected under the reporter's shield embodied in both Article I, section 2(b) of the California constitution and in California Evidence Code Section 1070" ; (2) the information was also protected by "the reporter's privilege under the First Amendment of the United States Constitution," which excused petitioners "from disclosing the source of any information procured in connection with [their] journalistic endeavors"; and (3) the subpoenas already issued against [two persons] could not be enforced without violating the Stored Communications Act (18 U.S.C. § 2702(a)(1)). In support of the motion, publishers each declared that they both had "received information about Asteroid contained in my article from a confidential source or sources."""[71]

The appeal court noted that news sites such as petitioners' reflected a kind and degree of editorial control that made them resemble a newspaper or magazine far more closely than they did the primordial discussion systems that gave birth to the term "post" by analogy to the physical bulletin boards they were named and patterned after.. It was they, and no one else, who "posted" the content of which Apple complains. The undisputed facts of record contradict any claim that unknown persons posted material on PowerPage.[72]

Article I, section 2, subdivision (b), of the California Constitution provides, "A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication...shall not be adjudged in contempt...for refusing to disclose the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public."[73]

The appeal court pointed out that shield is intended to protect the gathering and dissemination of news, and that is what petitioners did. It could think of no workable test or principle that would distinguish "legitimate" from "illegitimate" news. Any attempt by courts to draw such a distinction would imperil a fundamental purpose of the First Amendment, which is to identify the best, most important, and most valuable ideas not by any sociological or eco-

[70] *Id*. at *1 & *3.
[71] *Id*. at *5.
[72] *Id*. at *14.
[73] *Id*. at *19.

> nomic formula, rule of law, or process of government, but through the rough and tumble competition of the memetic marketplace.[74]
>
> Next, the appeal court analyzed whether the phrase "newspaper, magazine, or other periodical publication" (Cal. Const., art. I. § 2, subd. (b)) applied to Web sites such as petitioners'.[75]
>
> The court held that the explicit inclusion of television and radio in the shield law does not imply an exclusion of digital media such as petitioners'. It was "technically" debatable whether petitioners' web sites constituted "periodical publication[s]" within the contemplation of the statute. It noted that the Online Dictionary for Library and Information Science, (<http://lu.com/odlis/odlis--e.cfm#electronicmagazine>) defines "electronic publication" to include Web sites.[76]
>
> Next the court analyzed whether the web publications were periodical. It held that it did not appear that petitioners' web sites were published in distinct issues at regular, stated, or fixed intervals. Rather, individual articles were added as and when they become ready for publication, so that the home page at a given time may include links to articles posted over the preceding several days. This kind of constant updating is characteristic of online publications but is difficult to characterize as publication at "regular intervals." However, many familiar print publications universally viewed as "periodicals" (or "periodical publications") do not appear with absolute regularity.[77]
>
> The court concluded that petitioners were entitled to the protection of the shield law, which precludes punishing as contempt a refusal by them to disclose unpublished information. As for the Constitutional Privilege and its availability to Online Journalists the court held: we can see no sustainable basis to distinguish petitioners from the reporters, editors, and publishers who provide news to the public through traditional print and broadcast media. It is established without contradiction that they gather, select, and prepare, for purposes of publication to a mass audience, information about current events of interest and concern to that audience[78]

[74] *Id*. at *20.
[75] *Id*. at *22.
[76] *Id*. at *25.
[77] *Id*. at *26.
[78] *Id*. at *27-28. In doing so the California court has extended the legal protections crafted for the press "to everyone, effectively stating that we can all play a role in keeping our leaders accountable. We are all journalists now," Michel Geist, *We are all journalists now*, THE TORONTO STAR, 5 July 2006 at <http://geistalljournalistsnow.notlong.com>.

5.4.1.1. First Amendment

The First Amendment of the U.S. Constitution states: "Congress shall make no law…abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." The way this amendment has been interpretates in U.S. case law makes it clear that the freedom of speech in the U.S. has few boundaries when compared to other countries.

Thus, American online newspapers should be on guard when allowing access for foreigners to their websites, even though American courts have held that the Internet promotes First Amendment values in the same way that the historical use of traditional public fora for speaking, handbilling, and protesting testifies to their effectiveness as vehicles for free speech.79 The latter could indicate that an online newspaper has only a minimum risk that an American court will enforce in U.S. a foreign court decision that contravenes with the U.S. case law on the First Amendment. The district court decision in the Yahoo case supports this view.[80]

5.4.1.2. Communications Decency Act of 1996 §230

That the free speech protection pursuant to the First Amendment is extremely broad is further evidenced by the fact that the Federal Government – opposite most other countries - has issued a statute that immunizes Internet Service Provider by a statute in the Communications Decency Act of 1996. Thus, an exception rule was made similar to the one in general defamation law where an entity that merely distributes a defamatory statement, such as a bookstore or newspaper stand cannot be held liable, unless it knew or had reason to know of the defamatory statement at issue, because it is under no obligation to verify the content of the publications it sells.[81]

The CDA states, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information of an interac-

[79] *American Library Association, Inc. v. United States*, 201 F.Supp.2d 401, 488 (E.D.Pa. May 2002).

[80] *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F.Supp.2d 1181 (N.D.Cal., November 7, 2001).

[81] *Cubby, Inc. v. CompuServe, Inc*, 776 F.Supp. 135, 140-141 (S.D.N.Y. 1991).

tive content provider"[82]… As for State law: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[83] 230(e)(2) define "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

In practice however, only a few number of online news-publishers are also access providers and thus covered by the immunizing statute. An example was Internet access provider AOL that published news with help of a subcontractor. AOL was dismissed from the case because of the statute.[84] In *Aquino v. Electriciti*,[85] defendant Internet service provider was immune in a case where it had distributed material placed by an anonymous individual that stated that plaintiffs were "ring leaders" of "international conspiracy" to further "Satanic Ritual Abuse' children and that plaintiffs engaged in kidnapping, cannibalism, and murder of anyone who stood in way of "international conspiracy."

5.5. Single Publication Rule & Retraction

In common law, the main rule on defamation and publication originate from the English case *Duke of Brunswick*.[86] In that case, the Duke discovered that

[82] 47 U.S.C. § 230(c)(1) "Protection for "good Samaritan" blocking and screening of offensive material". *Carafano v. Metrosplash.com, Inc*., 207 F.Supp.2d 1055, 1064-1068 (C.D.Cal. 2002) (Discussed the range of "interactive computer service" provider and "information content" in the Act).

[83] 47 U.S.C. § 230(c)(3).

[84] *Sidney Blumenthal v. Matt Drudge*, 992 F.Supp. 44 (D.D.C. 1998). See also *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997) (Bulletin board) and *Doe v. AOL*, 783 S.2d 1010 (Supreme Court of Florida, 2001) (Chat room).

[85] *Aquino v. Electriciti Inc*., 26 Med.L.Rptr. 1032 (Cal. Superior, Sep. 1997) (Usenet newsgroup).

[86] *Duke of Brunswick v. Harmer*, 117 Eng. Rep. 75, 14 Q.B. 185 (Q.B. 1849) (Eng. Queens Bench, 1849).

a libel, published eighteen years previously, was in current circulation. The Duke bought from the publisher a copy of the original newspaper containing the libel. The Queens Bench held that the sale to the duke was a "fresh"[87] publication giving rise to a new cause of action. "Publication" in this context is the technical term in the law of libel meaning the communication of the defamatory matter to a third party who understands it.[88] Thus, the rule was established that each delivery and sale of an article containing defamatory material is a publication, which, defenses aside, gives rise to a separate cause of action. Under this law the publisher of a newspaper or periodical with a national circulating contain the fatal utterance could be subjected to as many suits as there are readers, rendering the statute of limitations completely ineffectual.[89]

5.5.1. Rules

First in the section different rules on publication will be mentioned as for the benefit of the reader, followed by illustrative cases together with comments on the rules' and case law's impact on online newspapers.

5.5.1.1. Restatement Tort (Second) section 577A

The "multiple publication" rule from *Brunswick* is still pursuant to Restatement (Second) Tort section 577A the starting point:

1. Except as stated in Subsections (2) and (3), each of several communications to a third person by the same defamer is a separate publication.
2. A single communication heard at the same time by two or more third persons is a single publication.
3. Any one edition of a book or newspaper, or any one radio or television broadcast, exhibition of a motion picture or similar aggregate communication is a single publication.
4. As to any single publication:

[87] *Id*. at 186.
[88] Lionel Rothkrug, *Defamation: Uniform Single Publication Act*, 44 CAL.L.REV 146, 147 and footnote 5 (1956).
[89] *Extraterritorial Jurisdiction*, 57 Ill.B.J. 672, 675 (1969).

- only one action for damages can be maintained;
- all damages suffered in all jurisdictions can be recovered in the one action; and
- a judgment for or against the plaintiff upon the merits of any action for damages bars any other action for damages between the same parties in all jurisdictions.

The rule was developed to simplify litigation by preventing multiple suits, thereby protecting the judicial system and defendants while preserving plaintiffs' rights to redress. In particular, it has been expanded to choice of law. "Rather than ascertain the appropriate substantive law for each claim comprising the composite action, courts extend the legal fiction so that they need only ascertain a single state's law to resolve the entire composite action. This ignores the fact that publication based torts are state created rights; application of a single state's law to determine all claims solely because they have been procedurally joined in a composite action encroaches on state sovereignty. It is also contrary to the purpose of substantive law." [90] In an attempt to administer these complex actions efficiently and conveniently, courts expanded the single publication rule to choice of law.[91]

5.5.1.2. Uniform Single Publication Model Act

The exception in subsection (2)-(4) of Restatement (Second) Tort section 577A is in practice equal to the wording of the Uniform Single Publication Model Act[92] of 1952:[93]

§ 1. [Limitation of Tort Actions Based on Single Publication or Utterance; Damages Recoverable]:

[90] Debra R. Cohen, *The Single Publication Rule: One action, not one law*, BROOKLYN LAW REVIEW, 62 Brook. L. Rev. 921, 924-926 (1996).

[91] *Id.*at 939-940.

[92] Both the Uniform Single Publication Act and the Restatement codify the law as it developed at common law, HANDBOOK OF THE NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS 430-31, Prefatory Note to the Uniform Single Publication Act (1952).

[93] Westlaw database: ULA SINGLE PUB.

"No person shall have more than one cause of action for damages for libel or slander or invasion of privacy or any other tort founded upon any single publication or exhibition or utterance, such as any one edition of a newspaper or book or magazine or any one presentation to an audience or any one broadcast over radio or television or any one exhibition of a motion picture. Recovery in any action shall include all damages for any such tort suffered by the plaintiff in all jurisdictions.

§ 2. [Judgment as Res Judicata]:

A judgment in any jurisdiction for or against the plaintiff upon the substantive merits of any action for damages founded upon a single publication or exhibition or utterance as described in Section 1 shall bar any other action for damages by the same plaintiff against the same defendant founded upon the same publication or exhibition or utterance.

§ 3. [Uniformity of Interpretation]:

This Act shall be so interpreted as to effectuate its purpose to make uniform the law of those states or jurisdictions which enact it.

§ 4:

This Act may be cited as the Uniform Single Publication Act.

§ 5. [Retroactive Effect]:

This Act shall not be retroactive as to causes of action existing on its effective date.

§ 6. [Time of Taking Effect]:

This Act shall take effect…

The Model Act has been basis for statutes in nine states, including California[94] whereas twenty-five have adopted the Single Publication Rule by case

[94] California Civ. Code § 3425, See further Appendix no. 3. On states, see Appendix no. 1.

law.[95]

Montana has explicitly rejected the single publication rule and continues to use the multiple publication rule;[96] and Wyoming's Supreme Court unlikely will adopt the single publication rule pursuant to the Tenth Circuit in *Anselmi*.[97]

Thus, there are big "holes" in the coverage of the Single Publication Rule since a total of 17 states either has rejected its use or are unsettled (Arkansas, Delaware, Hawaii, Indiana, Iowa, Kentucky, Maine, North Carolina, Oregon, Rhode Island, South Carolina, South Dakota, Utah, West Virginia, and Wisconsin).

5.5.1.3. Retraction

In an attempt to achieve the proper balance between the constitutionally protected guarantees of free expression and the need to protect citizens from reputational harm the National Conference of Commissioners on Uniform State Laws (NCCUSL)[98] in 1993 drafted the "Uniform Correction or Clarification of Defamation Act."[99] The Act, which applies to all defamations, whether public or private, media or non-media, is based on the following considerations:[100]

- Harm to reputation can often be cured by other than money damages. The correction or clarification of a published defamation may restore the person's reputation more quickly and more thoroughly than a victorious conclusion to a lawsuit.

[95] Partly from Reporters note to Section 577A of Restatement (2nd) Tort. On states, see Appendix 2.

[96] *Lewis v Reader's Digest Ass., Inc.* 512 P.2d 702, 704 (Mont. 1973) (The rule "is wrong in principle and in practice creates far graver problems that it solves.").

[97] *Anselmi v. The Denver Post, Inc*., 552 F.2d 316, 325 (10th Cir. 1977) ("[T]he single publication rule has not been adopted in Wyoming and is unlikely to be adopted").

[98] http://www.law.upenn.edu/bll/ulc/ulc_frame.htm> (visited April 2006).

[99] <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/uccda93.htm> (visited April 2006). Reprinted in Appendix 4.

[100] Prefatory Note to NCCUSL's draft of May 1, 1994 at <http://www.law.upenn.edu/library/ulc/ulc_frame.htm> (visited October 2004). See further Appendix 4.

- Secure quick and complete vindication of his or her reputation.
- The Act provides publishers with a quick and cost-effective means of correcting or clarifying alleged mistakes and avoiding costly litigation.
- In this way, both reputational interests and rights of free expression are advanced.

The Model Act requires in broad terms:

- The injured person must make a request for correction or clarification of a specified statement within 90 days after knowledge of the publication – or he may only recover provable economic loss.
- If a sufficient correction or clarification is made within 45 days the injured person may recover only provable economic loss, as mitigated by the correction or clarification
- The correction or clarification has to be published with a prominence and in a manner and medium reasonably likely to reach substantially the same audience as the publication complained of – with a copy to the person that made the request.

Retraction statutes have been made in some states, including Alabama[101] and California.[102]

5.5.2. US case law related to Single Publication Rule

The content of the Model Single Publication Rule gives rise to at least the following questions that have an impact on its usefulness for the online environment:

- What circumstances pursuant to the Rule bar further claims?
- What circumstances will start a new Single-Publication-period?

The following will give a brief overview to some case law that might have effect on online newspapers. The cases in the context of the Internet are dealt with in section 5.7 below.

[101] Alabama Code §6-5-186 on Prerequisites to recovery of vindictive or punitive damages in action for libel, see Appendix 5.

[102] California's Civil Code § 48a on Libel in newspaper; slander by radio broadcast. See further Appendix 6.

As to the latter question, the *Kanarek*[103] case gives some indication. Plaintiff had initially sued for damages causes by an alleged libelous book issued in hardcover. That case was dismissed for different reasons, including exceeding time limits. After the book was republished in paperback, the plaintiff sued again. The court held that the paperback edition "undoubtedly intended to and did reach a new group of readers" and therefore found it was a new action for damages that was not barred by the Single Publication Rule.[104] The court noted a new cause of action for libel does not arise each time a new reader purchases the material.[105]

Thus, "if the same defamatory statement is published in the morning and evening editions of a newspaper, each edition is a separate single publication and there are two causes of action. The same is true of a rebroadcast of the defamation over radio or television or a second run of a motion picture on the same evening. In these cases, the publication reaches a new group and the repetition justifies a new cause of action."[106]

On the other hand, "printing and distribution of extra copies of the first edition of a book is mere continued circulation of the first edition and hence still part of the first (single) publication, if it is done not long after the original publication as soon as the supply is exhausted."[107]

Defendant in *Swafford*[108]- a case of first impression - argued that, once information was stored on an electronic database, it becomes openly accessible to the public and is akin to the "circulation of copies of an edition of a book, newspaper, or periodical" pursuant to the Single Publication Rule. Thus, it contended that any alleged injury occurs at the time the information is stored in the database. Plaintiff argued that injury does not occur until the information stored in the database is requested and retrieved by individual with ac-

[103] *Kanarek v. Bugliosi*, 108 Cal.App.3d 327, 166 Cal.Rptr. 526, 6 Media L. Rep. 1864 (Cal.App.2.Dist. 1980).
[104] *Id*. at 333 or 530.
[105] *Id*. at 332 or 529.
[106] Comment d to Restatement (Second) Tort section 577A *quoted* by *Swafford v. Memphis Individual Practice Ass*, 1998 WL 281935 at *4, 1998 Tenn.App. LEXIS 361 (Tenn.Ct. App.1998).
[107] *Id*. Comment d.
[108] *Swafford supra* note 106.

cess to the base.

The court pointed out, that the National Practitioner Data Bank, whereto defendant had stored an alleged libelous report, operated pursuant to a Federal statute, was maintaining information concerning health care providers, was confidential, and could be accessed only by health care entities.[109] It held the confidential nature of the report necessarily meant that each transmission of the same credit report was a separate and distinct tort to which a separate statute of limitations applied.[110]

Unlike the mass publication of a book, magazine, or television commercial, the information stored in the Data Bank was not within the domain of the "contemporary publishing world," but only accessible for special entities – not the general public - upon separate and distinct requests. Therefore, there was no "aggregate publication" as contemplated in cases applying the single publication rule. Thus, the justification for the single publication rule, namely a vast multiplicity of lawsuits resulting from a mass publication, was not present here. Therefore, a separate limitations period attached to each request,[111] that is the multiple publication rule applied to the disseminations of an online medical service.

In *Firth*[112] a unanimous seven panel decided in a case of first impression on whether the single publication rule is applicable to allegedly defamatory statements that are posted on an Internet site and, if so, whether an unrelated modification to a different portion of the Web site constitutes a republication.

At a press conference, the Office of the State Inspector General issued a report, which was critical of claimant's managerial style and procurement of weapons. On the same day plaintiff's former employer posted an executive summary with links to the full text of the report on its Government Information Locator Service Internet site. The link enabled users to download or view

[109] *Id*. at *1.
[110] *Id*. at *6
[111] *Id*. at *8 and footnote 8.
[112] *Firth v. State of New York*, 98 N.Y.2d 365, 775 N.E.2d 463, 747 N.Y.S.2d 69, 30 Media L. Rep. 2085 (N.Y. 2002), *followed* by the Second Circuit in *Van Buskirk v New York Times*, 325 F.3d 87 (2nd Cir.)(holding that plaintiff's claim was time-barred because the single publication rule applied to a letter published on defendant newspaper's website).

the text of the report. More than one year after plaintiff filed a claim against the State alleging that the report defamed him.

The court rejected that the single publication rule should not be applied to defamatory publications posted on the Internet in light of significant differences between Internet publications and traditional mass media. Further, it rejected arguments that because its publisher or owner may alter a web site at any time and because publications on the Internet are available only to those who seek them, each "hit" or viewing of the report should be considered a new publication that retriggers the statute of limitations.[113]

It noted, "[r]epublication, retriggering the period of limitations, occurs upon a separate aggregate publication from the original, on a different occasion, which is not merely 'a delayed circulation of the original edition.'"[114]

The court held "the mere addition of unrelated information to the web site could not be equated with the repetition of defamatory matter in a separately published edition of a book or newspaper", since "the justification for the republication exception has no application at all to the addition of unrelated material on a web site, for it is not reasonably inferable that the addition is made either with the intent or the result of communicating the earlier and separate defamatory information to a new audience."[115]

It pointed out, that many web sites are in a constant state of change, and that web sites are used by news organizations to provide readily accessible records of newsworthy events as they occur and are reported. Otherwise, a publisher would be forced to either avoid posting on a web site or use a separate site for each new piece of information, which would discourage or slow down the unique information advantages by the Internet. This militated against a holding that any modification to a web site constitutes a republication of the defamatory communication itself.[116] Furthermore, the court held that the one-year statute of limitation in New York runs from the first posting of defamatory matter upon an Internet site.[117]

However, in a successive suit a lower New York court between the same

[113] *Id*. at 369 and 465.
[114] *Id*. at 371 and 466.
[115] *Id*. at 371 and 466.
[116] *Id*. at 372 and 467.
[117] *Firth* at 369, see footnote 112. See also §577A of the Restatement of Torts, 2d, (1977).

parties refused to dismiss the case on ground of statute of limitations since the defendant state had moved the report to a news directory on the State Library's web site as part of defendant's web site revision project. The court held the reports move to a different Internet address were sufficient to state a cause of action for republication to a new audience akin to the repackaging of a book from hard cover to paperback.[118]

In *Simon,* the court emphasized that the allegedly libelous article was available to the public from the time it was uploaded to the Web and that local Mountain Standard Time was determining.[119] As for the limitation statute, it did not matter that the same article was published in a (first coming) print version with a date one day later.[120]

5.6. Cases with foreign aspects

Choice of law or conflicts of law will not be discussed in the following, as there exist different approaches in each nation's choice of law-conflict of law rules. Generally, the Continental thinking about adjudicatory jurisdiction stresses indirect affiliations between the parties and the forum that arise from the underlying controversy; whereas the traditional Anglo-American thinking about adjudicatory jurisdiction has concentrated on direct affiliations - in particular, presence and domicile[121] - between the parties and the forum; thus,

[118] *Firth v. State of New York*, 306 A.D.2d 666, 761 N.Y.S.2d 361 (N.Y.A.D. 3.Dept. 2003).

[119] *Simon v. Arizona Board of Regents*, 28 Med.L.Rptr. 1240, 1246 [1] (Ariz.Sup. 1999).

[120] *Id*. at 1242

[121] In the legal systems of other civilized states than the Anglo-American there is a conception of domicile which, although it may differ in details fro the common-law conception, in its broad outlines is the same. The generally accepted rules for ascertaining a person's domicile in states where the Anglo-American common law prevails are pursuant to §10 of RESTATEMENT (FIRST) OF CONFLICT OF LAWS: (1) A question of domicile as between the state of the forum and another state is determined by the law of the forum. (2) A question of domicile as between one or another of several states other than the forum, the law of each of which differs from that of the other and from that of the forum, is determined by the law of the forum.

these notions tend to dissociate jurisdiction and choice of law.[122]

5.6.1. Malaysia

A very special matter occurred in a Malaysian case. The Malaysian court refused to deal with a defamatory statement in a Singapore newspaper also available on Internet. The alleged libel, published in the *Strait Times* and the *Business Times*, was printed and for publication and sale in Singapore, and also published in an online version.

The courts refusal was based on the fact that neither the paper version nor the online version as required by Malaysian law was authorized to be imported, sold, circulated or distributed in Malaysia. The court held that even if persons in Malaysia had access and read the online version such access had not been allowed by Malaysia. Thus, the statement was not regarded as published in Malaysia, there could not be committed a tort in Malaysia.[123]

5.6.2. Canada

A lower Canadian court in 2004[124] refused to dismiss on lack of jurisdiction a case involving American Washington Post since a defamatory[125] statement was available in Canada through the Internet.

In 1997, when Guinean-born and Guinean national Cheickh Bangoura worked for the United Nations in Kenya, the Washington Post published two articles relating to Bangoura's conduct in a previous UN posting on the Ivory Coast. The newspaper had no wholesale distribution in Canada[126] and had only seven paid subscribers in Ontario. The articles were freely available

[122] SPANG-HANSSEN-2 *supra* note 28 at 445; Arthur T. von Mehren & Donald T. Trautman, *Recognition of Foreign Adjudications: A Survey and a suggested Approach*, 81 HARV. L. REV. 1601, 1636-38 (1968).

[123] *Lee Teck Chee v. Merrill Lynch International Bank Ltd*., [1998] 4 CLJ 188 (High Court Lalaya, Kuala Lumpur (Malaysia), 26 February 1998 - Civil No. S2-23-51-1997).

[124] *Cheickh Bangoura v. Washington Post*, 2004 CarswellOnt 340, 2004 WL 95104, 2004 A.C.W.S.J. LEXIS 307, 2004 A.C.W.S.J. 1383, 128 A.C.W.S. (3d) 478 (Ontario Superior Court of Justice, January 27 2004) [hereinafter *Bangoura 2004*].

[125] *Cheickh Bangoura v. Washington Post*, 2005 CarswellOnt 4343 paras 18 (Ontario court of Appeal, September 16 2005) [hereinafter *Bangoura 2005*].

[126] *Bangoura 2004 supra* note 124.

online for 14 days after publication, but thereafter only accessible through a paid archive.[127]

Six years after publication, and almost three years after moving from Africa to the Canada as an immigrant in 1997, Bangoura raised proceedings in an Ontario court against both the newspaper and three of its reporters, seeking an injunction, a retraction and $10 million in damages. He became a Canadian citizen in 2001 and had the last two years lived in Ontario where he now worked.[128]

In January 2004, Ontario's Superior Court of Justice ruled that it had jurisdiction to hear the case.

Washington Post's main argument was the case "New York Times Co. v. Sullivan, 376 U.S. 254 (1964) where the U.S. Supreme Court refused to enforce a British libel-judgments on the ground that British libel law is repugnant to the policies of the U.S.A."[129]

The lower Canadian court pointed out that it did "not share the American view that British libel law, which is similar to our own, is any less civilized than the American law, See Hill v. Church of Scientology, [1995] 2.S.C.R. 1130 at 1187-88, Cory J. The Supreme Court of Victoria (Australia) does not share the American view either." The court largely quoted from the Australian case, which is mentioned below under Australia. It noted that in the context of allegedly false and injurious communications over the Internet, the location of the plaintiff is a key factor that receives greater weight than other factors. This is the case because damage to the reputation and actual pecuniary loss is the key element in such an action, and a plaintiff will experience damages most keenly in the jurisdiction in which they reside.[130]

In addition it remarked that the Washington Post defendant's home jurisdiction's unwillingness to enforce such an order is not determinative of whether the court should assume jurisdiction.[131]

The newspaper and its reporters appealed.

The Ontario Court of Appeal unanimously reversed and held Ontario

[127] *Bangoura 2005 supra* note 115, at paras 1 and 11.
[128] *Bangoura 2004 supra* note 124, at para 7-8.
[129] *Bangoura 2004 supra* note 124, at para 21 at (8) .
[130] *Bangoura 2004 supra* note 124, at para 22 at (f) .
[131] *Bangoura 2004 supra* note 124, at para 23.

courts did not have jurisdiction to hear the case.[132]

The court distinguished the circumstances from those of Joseph Gutnick who raised a claim in Australia over a US publication. Gutnick was a well-known businessman who resided in Victoria at the time of the impugned publication…and there was evidence that Barron's had some 1,700 Internet subscribers in Australia. Gutnick undertook that he would sue only in Victoria and only in respect of damages to his reputation in that state.[133]

The Canadian Appeal court held that the connection between Bangoura's claim and Ontario was "minimal at best",[134] and there was no evidence that Bangoura had suffered significant damages in the province.[135] Furthermore, it was not reasonably foreseeable in January 1997 that Mr. Bangoura would end up as a resident of Ontario three years later. To hold otherwise would mean that a defendant could be sued almost anywhere in the world based upon where a plaintiff may decide to establish his or her residence long after the publication of the defamation.[136] Furthermore was noted, that there was no evidence that the Washington Post had insurance coverage in Ontario.[137]

The courts pointed out, that where the case is international in nature, rather than interprovincial, it is more difficult to justify the assumption of jurisdiction.[138]

On February 16, 2006, the Supreme Court of Canada refused leave to appeal.[139]

[132] *Bangoura 2005 supra* note 115, at para 46.
[133] *Bangoura 2005 supra* note 115, at paras 43-44. *See Gutnick v. Down Jones* below in section 5.6.4, Australia.
[134] *Bangoura 2005 supra* note 115, at para 22.
[135] *Bangoura 2005 supra* note 115, at para 23.
[136] *Bangoura 2005 supra* note 115, at para 25.
[137] *Bangoura 2005 supra* note 115, at para 27.
[138] *Bangoura 2005 supra* note 115, at para 35.
[139] *Cheickh Bangoura v. Washington Post*, 2006 CarswellOnt 932 (Supreme Court of Canada, February 16, 2006 – Docket 21203).

5.6.3. United Kingdom

The US Single publication rules has no support in English law[140] since the rule is contrary to the long established principle of English libel law that each publication is a separate tort. An English court has noted that each "hit" on an online archive of previous published material effectively amounts to a republication, and the limitation period runs from the time the material was accessed.[141] "Moreover, the rule is inconsistent with the policy underlying the acceptance by the European Court of Justice in" *Shevill*. This court stated that an Internet publication takes place in each country in which the material is downloaded, irrespective of where the server is based.[142]

The House of Lords in *Berezosky v. Forbes* noted about an on-line version of a magazine on the Internet and the jurisdiction that there was not the necessary evidence before the House to consider this important issue satisfactorily. Thus, the availability of the article on the Internet was, opposite the lower court,[143] not discussed.[144]

In *Don King*[145] the High Court noted that "it has long been recognized that publication is regarded as taking place where the defamatory words are published in the sense of being heard or read…by analogy, the common law

[140] *Berezosky v. Michaels & Berezosky v. Forbes*, [2000] E.M.L.R. 643, 653, [2000] 2 All ER 986, [2000] 1 WLR 1004, 2000 WL 544123 (House of Lords, May 2000) and *Loutchansky v. The Times Newspapers Ltd.*, [2001] EWCA Civ 1805 para 72, [2002] 1 All ER 652, <http:// www.bailii.org/ew/cases /EWCA/Civ/2001/1805.html> (England and Wales Court of Appeal, 5th December, 2001) (newspapers placed in an online archive).

[141] *Loutchansky supra* note 140, at 74-75.

[142] *Shevill v.Presse Alliance SA*, [1995] 2 A.C. 18, 1995 E.C.R. I-415, [1995] E.M.L.R. 543, (E.C.J. Case C-68/93, 1995) & LAW COMMISSION, DEFAMATION AND THE INTERNET 21, 27-39 (UK, December 2002) <http://www.lawcom.gov.uk/239.htm#1lcr266 (visited October 2003) or http://www.lawcom.gov.uk/files/defamation2.pdf.

[143] *Berezovsky v. Forbes Inc*., [1999] I.L.Pr. 358 para 37, 1998 WL 1043805, [1999] E.M.L.R. 278, (English Court of Appeal, 1998).

[144] *Berezosky v. Michaels & Berezosky v. Forbes*, [2000] E.M.L.R. 643, 657.

[145] *Don King v. Lennox Lewis, Lion Promotions, L.L.C. & Judd Burstein*, [2004] EWHC 168 para 15, 2004 WL 62126 (High Court of Justice Queen's Bench Division 6 February 2004) *affirmed* by Court of Appeal (Civil Division) in [2004] EWCA Civ1329 (19. October 2004).

currently regards the publication of an Internet posting as taking place when it is down-loaded." The case dealt with a "trans-national libel"[146] in stories published on two American websites. All parties were Americans and it was noted that an equal action in a New York court would not have been possible because of New York law on public figures. Defendant argued plaintiff was forum shopping. The English Court of Appeals noted that it "makes little sense to distinguish between one jurisdiction and another in order to decide which the defendant has "target", when in truth he has "target" every jurisdiction were his text may be downloaded."[147] It held England was an "appropriate" forum.

The same High Court in *Schwarzenegger*[148] asserted jurisdiction over an Internet libel suit launched against California Governor Arnold Schwarzenegger. The suit arose from an article in the LA Times available online that discussed an alleged sexual harassment. The court applied the *Don King* decision in determining that an "internet publication takes place in any jurisdiction where the relevant words are read or downloaded." Plaintiff, a Hollywood publicist, had limited her claim to publication happening in England and Wales.

> On 26 June 2006 the British Highest Court, the House of Lords[149] heard the appeal of *Yousef Jameel v Dow Jones*,[150] which deal with a libel-claim on a Saudi businessman in respect of an article published on an internet website, which was said on behalf of the claimant to be available to between five and ten thousand subscribers within the jurisdiction. The claimant invited the inference to be drawn that a substantial number of readers of the main article would have read the page to which the hyperlink led. The defendant publishers adduced evidence that only five subscribers within the jurisdiction had

[146] *Id.* [2004] EWCA Civ1329 para 28.
[147] *Id.* para 34.
[148] *Anna Richardson v. Arnold Schwarzenegger*, *Sean Walsh and Sheryl Main* [2004] EWHC 2422 (High Court, Queens Bench Division, October 29 2004 – case no. HQ04X01371). *See also*, Case Comment: *Arnold Schwarzenegger Case not Terminated*, 2005 ENTERTAINMENT LAW REVIEW, 16(6), 156-158.
[149] Frances Gibb, *Law lords to rule on internet defamation*, TIMES ONLINE, 26 June 2006 at <http://www.timesonline.co.uk/article/0,,200-2243300,00.html>.
[150] *Yousef Abdul Latif Jameel v Dow Jones & Co Inc.,* [2005] 2 WLR 1614, [2005] Q.B. 946, [2005] E.M.L.R. 16, [2005] EWCA Civ 75 (Court of Appeal, 3 February 2005).

been able to access the alleged libel via the hyperlink. Of those five, three were members of the claimant's "camp". The Court of Appeal struck out the claim as an abuse of process on the ground that the extent of the publication within the jurisdiction was minimal and did not amount to a real and substantial tort.

The *Jameel* case was relied upon by the court in *Amoudi v. Brisard*[151] where the issue was whether and, if so, in what circumstances it is open to a claimant complaining of an item on an Internet website open to general access to rely on a presumption that substantial publication of that item has taken place within the jurisdiction of the court.
Plaintiff was described as a prominent and respected international businessman who was well known in the major financial centres of the world, including London. He was born in Ethiopia but has made his home in Saudi Arabia. He was said to spend a total of approximately two to two-and-a-half months a year in England for business and personal reasons. He has a home in London. The first Defendant, M. Brisard, who was a French national resident in Switzerland, asserted that he was an author and international expert and investigator on terrorism financing. The second Defendant was a limited liability Swiss company of which M. Brisard was the managing partner, the majority shareholder and one of the two authorised signatories. The company was said by M. Brisard no longer to be in existence. The claim was in respect of two publications.
Justice Gray remarked that proof that Internet communications have been published is [] not usually a difficult task.[152]
He found assistance on the question raised before him could be derived from Jameel v Dow Jones Inc [2005] 2 WLR 1614 (Court of Appeal) as it appeared to him "to be of some significance that there was no suggestion made on behalf of the claimant in the context of that case that he could rely on any presumption of publication. The fact that the Court of Appeal struck out the claim provides some support for the view that an argument in favour of the

[151] *Mohammed Hussein al Amoudi v. (1) Jean Charles Brisard & (2) JCB Consulting International Sarl*, [2006] EWHC 1062 (England and Wales High Court (Queen's Bench Division – Justice Gray), 12 May 2006) also at <http://www.bailii.org/ew/cases/EWHC/QB/2006/1062.html>

[152] *Id.* at para 35 and making reference to his judgment in *Loutchansky v Times Newspapers Ltd (No 2)* [2001] EMLR 876 and MATTHEW COLLINS, THE LAW OF DEFAMATION AND THE INTERNET section 5.04 (2nd Edition - Oxford University Press).

> existence of a presumption of publication would not have found favour with the court."[153]
>
> The only documents which were disclosed by the Defendants in relation to the number of hits on the website were monthly summaries of the number of hits said to have been recorded broken down by country. The court held the provenance of those summaries was unclear. On the face of them it appeared that the number of hits made on the website from the United Kingdom had been few. The summaries did, however, record a large number of hits where the country from which they were made was either not known or not recorded. The court held it was an open question whether some at least of these unsourced hits had been made from the court's forum.
>
> Justice Gray held that he was "unable to accept that under English law a claimant in a libel action on an Internet publication is entitled to rely on a presumption of law that there has been substantial publication."[154]

Thus, plaintiff should count the readers before suing for internet libel in England, unless the *Jamell* appeal case overturns *Amoudi*.

5.6.4. Australia

In the Australian case *Gutnick v. Down Jones* (see also above section 5.6.2., Canada), a case dealing with issues of the single publication rule, jurisdiction and choice of law, the lower court rightly pointed out that "this is a subscription website,"[155] thus a website made for gaining profit. The court noted that the "case is not concerned with the world wide web because Dow Jones only puts it on for subscribers or trial subscribers."[156] That puts the case with respect of the personal jurisdiction question into the group of US Cyberspace cases, where defendant is doing business in the forum. Thus, this was not a case concerning the free Internet, as it does not dealt with the issue of a "publisher" that acts as an intermediary for third person who makes the defamatory statement. Neither does the case deal with the issue of a "publisher" being sued by a person, who is not the "target" for the defamatory state-

[153] *Id.* at para 36.
[154] *Id.* at 37.
[155] *Gutnick v. Dow Jones & Co, I*nc, [2001] VSC 305 para 14, 2001 WL 966287 (Supreme Court of Victoria (Australia) Aug, 2001 - NO. 7763 of 2000) at <www.austlii.edu.au/au/cases/vic/VSC/2001/305.htm> (visited August 29, 2001).
[156] *Id.* para 41.

ment.[157]

Rather, the case dealt with the question of where the tort of defamation is committed if the place in which the publisher acts and the place in which the publication is presented in comprehensible form are in two different jurisdictions. Australia's highest court[158] - in a unanimous decision - found "[i]n the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. [Further, i]t is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed."[159]

Australia's highest court[160] unanimous rejected the U.S. "single publication" rule and noted this rule said "nothing about the question of jurisdiction."[161] It pointed out that the U.S. Single Publication Rule had extended from a time limiting rule to be also a rule of choice of law, which was not acceptable[162] amongst others because tort law might be different in different States or territories.[163]

The court noted that defamation is to be located at the place where the damage to reputation occurs.[164] The court noted that those who make information accessible by a particular method do so knowing of the reach that

[157] Spang-Hanssen to "Net defamation" in AUSTRALIAN IT, August 29, 2001 at <http://australianit.news.com.au/common/story-PAGE/0,3811,%202783041% 255E506,00.html> (visited September 2001).

[158] *Dow Jones v. Gutnick*,[2002] HCA 56 paras 28, 42 & 44, 42 I.L.M. 41, 2002 WL 31743880, 210 CLR 575, 194 ALR 433, 77 ALJR 255, [2003] AIPC 91-842 (High Court of Australia, 10 December 2002 - No. M3/2002) <http:// www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html> (visited 10 December 2002). In a out-of-court settlement of November 2004, Gutnick was awarded $180,000 and in cost $400,000, *Gutnick 'delight' on defamation deal*, THE AUSTRALIAN, November 12, 2004 at <http://www.theaustralian.news.com.au/common/ story_page/0,5744,11365187%255E1702,00.html> (visited November 15, 2004).

[159] *Id.* para 44.

[160] *Id*. at para 28, 42 & 44.

[161] *Id.* at para 36.

[162] *Id*. at para 32.

[163] *Id*. at para 37.

[164] *Id*. at para 44.

their information may have: "In particular, those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction."[165]

In a concurring judgment, Justice Callinan stated: "A publisher, particularly one carrying on the business of publishing, does not act to put matter on the Internet for it to reach a small target. It is its ubiquity which is one of the main attractions to users of it... Publishers are not obliged to publish on the Internet. If the potential reach is uncontrollable then the greater the need to exercise care in publication."[166] This does not mean that publishers will be faced with uncertainty and the possibility of being sued in any jurisdiction in the world for each publication.

The court noted, "[t]hose who would seek to order their affairs in a way that will minimize the chance of being sued for defamation must be able to be confident in predicting what law will govern their conduct. But, certainty does not necessarily mean singularity. What is important is that publishers can act with confidence, not that they be able to act according to a single legal system, even if that system might, in some sense, be described as their "home" legal system."[167]

5.6.5. United States

In *Dow Jones v. Harrods,*[168] the owner of American Wall Street Journal tried to avoid a potential libel lawsuit in United Kingdom based on alleged damaging content from a newspaper article that was also made available on the Journal's website to which subscribers had access. After London based Harrods had brought suit in English court, Dow Jones amended its complaint in the New York court to seek an anti-suit injunction barring Harrods from suing in the U.K. Harrods moved for dismissal in the US court. The Second Circuit affirmed the districts courts holding that:

- the action was non-justifiable because it was not ripe for adjudication;

[165] *Id*. at para 39.
[166] *Id*. at paras 181-182.
[167] *Id.* at para 24.
[168] *Dow Jones v. Harrods*, 346 F.3d 357 (2nd Cir. Oct 2003).

- there was no "actual controversy" as required by the Declaratory Judgment Act, 28 U.S.C. 2201; and
- the court would decline to exercise its jurisdiction to hear the case under the Act on the grounds that no useful purpose would be served by a declaration and that principles of international comity would be violated.

In *Young*[169] the Fourth Circuit reversed the lower courts decision and dismissed the case because it held that a court in Virginia could not constitutionally exercise jurisdiction over the Connecticut-based newspaper defendants since they did not manifest an intent to aim their websites or the posted articles at a Virginia audience.

The Appeal court emphasized how important it is in light of Calder to look at whether the defendant has expressly aimed or directed its conduct toward the forum state. It held that "although the place that the plaintiff feels the alleged injury is plainly relevant to the [jurisdictional] inquiry, it must ultimately be accompanied by the defendant's own [sufficient minimum] contacts with the state if jurisdiction ... is to be upheld."

The Circuit court pointed out that "the fact that the newspapers' websites could be accessed anywhere, including Virginia, does not by itself demonstrate that the newspapers were intentionally directing their website content to a Virginia audience. Something more than posting and accessibility is needed to "indicate that the [newspapers] purposefully (albeit electronically) directed [their] activity in a substantial way to the forum state," Virginia."[170]

"The newspapers must, through the Internet postings, manifest an intent to target and focus on Virginia readers."

5.7. The issue related to the Internet

The just above-mentioned U.S. case shows the schism especially online newspapers have. With the present computer technique, it is impossible for

[169] *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir. Dec. 13, 2002), *certiorari denied* in *Young v. New Haven Advocate,* 538 U.S. 1035, 123 S.Ct. 2092 (US Supreme Court, May 19, 2003 – Doc. 02-1394).

[170] *Id.* 315 F.3d 256, 263.

them to bar themselves from lawsuits anywhere as the online contents can be read everywhere and by everyone. The American *iCraveTV* case[171] is a good example of a Canadian company trying to comply with Canadian law and to avoid liability in foreign countries.

The result of the American court's rejection of accepting the *Harrods* case[172] is that the American online newspaper must wait until a British court has issued a decision against it as an defendant and then at the time of enforcement hereof argue that the libel suit should not have been decided by a British court and should not be enforced in the U.S. However, holdings such as the one in *Harrods* can become devastating for online business as evidenced by the Yahoo-dilemma, where Yahoo as of December 2004 has accumulated somewhat 250 million dollars in French penalties - an amount that can bring most newspapers into bankruptcy.

As for plaintiffs, it seems to be a waist of time and money to get their local courts to decide a libel suit as in the *Don King* and *Schwarzenegger* cases,[173] which system also was followed by the lower court in the Canadian *Bangoura* case,[174] where the lower court noted it was aware of the fact that the decision might be a dead letter as the court knew its decision probably not would be enforced by U.S. courts. The problem with enforcement will probably be the same as for the *Don King* and *Schwarzenegger* cases.

The only reel "enforcement" threat that plaintiffs with a foreign court decision have seems to be the threat that the defendant might be arrested upon arrival in the country of the court decision. Thus, if an American court respectively an EU-member state court has issued a decision against a foreign defendant, that defendant will not without a risk of being arrested dare to travel to United States respectively the EU-states as both group of states' courts are obliged to enforce each groups decisions and thus arrest persons arriving into the groups' territory. Thus, Schwarzenegger cannot go to visit his family in Austria of fear of being arrested based on an UK decision that might not be enforceable in US, because of enforcement-rules between the

[171] See footnote 63.
[172] See footnote 168.
[173] See footnotes 145 and 148.
[174] See *Bangoura 2004 supra* note 124 (the decision was reversed by the Appeal court, see footnote 125) .

E.U. member states.

As newspapers base their business on collecting news from around the world, it will be devastating for their business if there exists areas around the world where they cannot collect news or make research or interviews to their "local" online newspapers because of the risk of being arrested in a foreign State caused by a previous local decision based on libel in the "foreign" online newspaper.

Another devastating aspect for online newspapers, as the *Don King* case[175] is an excellent example of, is that courts seem to be willing to allow forum shopping. That case involved only American parties and a case where the plaintiff would not be able to achieve damages in United States (New York).

A more general question is, what is a online newspaper, when confronted with the fact that most Internet Access Providers also bring news collected from "real" newspapers, and the fact that most online newspapers does not have subscribers as is the case of paper-version-newspapers.

Distribution of news on the Internet can be divided into:[176]

- Subscribers pays all
- Advertisers pays all
- Subscribers pay some, advertisers pay some

Dictionaries[177] define a "newspaper" as a printed publication usually issued daily or weekly and that contains news, articles of opinion, and advertising. However, for online newspapers, the latter of this definition seem to have become the sole business for most online newspapers. For example, in 1999, abandoning its 10-month attempt to attract subscribers at $19.95 annually, Slate's publisher – a Microsoft funded online magazine – wrote "that by making Slate free our audience will grow substantially and this will make us more attractive to advertisers." On the Web, "paid subscriptions for content

[175] See footnote 145.

[176] BENJAMIN M. COMPAINE & DOUGLAS GOMERY, WHO OWNS THE MEDIA – COMPETITION AND CONCENTRATION IN THE MASS MEDIA INDUSTRY 446 (Chapter 7 "The Online Information Industry" by Benjamin M. Compaine) (Lawrence Erlbaum Associates, Publishers, Third Edition, 2000 – ISBN 0-8058-2935-0) [hereinafter COMPAINE].

[177] Merriam-Webster's Collegiate Dictionary (11th Edition 2003) and Oxford Talking Dictionary. (1998).

(other than smut and investments) simply have not grown as expected."[178]

Reuters was first of the news services in the online world and became the only or primarily source for the news articles that were available on the home pages of the millions of users of Lycos, Excite, Netscape, Yahoo and Info-Seek.[179] Otherwise for Associated Press (AP), that feared undercutting its value to its client/owners (a cooperative of some 1550 newspapers). First in 1996, AP introduced "The Wire," which essentially gave individual web users access to AP stories through its own site. Public access to the AP is just one example of how the Internet may be able to remove layers of gatekeepers to news and information.[180]

Thus, a big segment of what fairly can be regarded as online news from the users perspective is in reality far from what is regarded as newspapers in the brick and mortar world, where newspapers are something the readers buy in newspaper-booths or subscribe to.

Furthermore, in the brick and mortar world newspaper-libel-cases were based on the fact that newspapers knew where they were doing business. Thus, the international society of states did not find it unreasonable for newspapers to have to defend themselves in courts where the reader was located, that is, where the defamation happened since tort requires the libel to be know by a third person. It should be remembered that the main elements of a defamation claim are:

- A false statement

[178] COMPAINE *supra* note 160 at 451, quoting Alex Kuczynski, *Slate Ends Its 10-month Experiment with Subscribtions*, THE NEW YORK TIMES, February 15, 1999 at <www.nytimes.com/library/tech/99/02/biztech/articles/15slat.html>. The critical role of the portal sites for the attention of users was bolstered by survey research that found "almost half of online users…access news via search engines or directory websites." The same research also suggested that consumers' preference for collecting news on these entry sites has also lead to another trend: As "search engines pull stories straight from the 'wires,' news services such as Associated Press, Bloomberg, and Reuters are becoming more familiar to consumers," COMPAINE *supra* note 160 at 460, quoting *Portals Emerge as Dominant Source for Online News*, New York, JUPITER COMMUNICATIONS, December 8, 1998, at <www.jup.com/jupiter/press/releases/1998/1208a.html>.

[179] COMPAINE *supra* note 170 at 467.

[180] COMPAINE *supra* note 170 at 463.

- Referring to the plaintiff
- Published to one or more third parties
- Causing damage to the plaintiff

However, the international society has never thought that a libel made in one country could be dealt with by any court in the world. But, this seems to be the present situation for most courts when keeping in mind the case law mentioned above. The case from Malaysia[181] is an exception as it held the decisive was whether the online newspaper had been registered doing business in that country. To a certain extent was "doing business" also the determining factor in the Australian lower court's decision in *Gutnick*[182] as that court emphasized the defendant had subscribers in Australia to the online newspaper. There seems to be a need for a special online news libel rule.

If one follows the above though of thinking and also keeping in mind that most online newspapers earn their money from advertising alone (without subscriber fee) the determining factor for where a libel is done – and thus where suits can be brought into court over online newspapers - should be:

- The place where the original electronic communication ("bits-transfer") was prepared, the communication was uploaded, or where the newspaper is located physical - as the plaintiff pursuant to international law always can sue in the offender's own country ("the sender's point of view", see above section 5.3.1)
- In the country(ies) where the advertising is being target – as this is where the online newspaper truly is doing business and thus a libel should be expected to be read by a third-party, which is required for the tort-action. ("the receiver's point of view", see above section 5.3.1)
- In the country(ies) where the online newspaper has subscribers. ("the receiver's point of view", see above section 5.3.1)

The above would secure the online newspaper pursuant to international law to have adequate notice of where to be sued for libel. The above prong B should not be totally an American "minimum contact" test (or rather an "effect test") as this would allow the court to take into consideration the "local

[181] See footnote 123.
[182] See footnote 155.

public interest" in the case. Rather, it should be an objective test where the content of the advertising should be the fact showing where an online newspaper is doing business.[183] In this respect language should be a determining factor in the negative as for example an online newspaper with advertising in French should only be sued for libel in territories where French language is the official language – and of course in countries where the online newspaper have subscribers. As for France should be noted that its own law requires this, as the Toulon law states any website targeting France for at least fifty percent has to be in French.[184]

As for the question of libel and editions of online newspapers, the starting point must be the situation, which is the basis in common law (and in most civil countries), that is, the rule from *Brunswick*[185] or the "multiple publication rule."[186] The multiple publication rule is based on the wish to allow the defamed person to file suit at his local jurisdiction or where the harm is really felt and each time the publication reach a new group of readers.

The only generally accepted exception around the world has been that one

[183] The reporter of Restatement (Third) of Foreign Law, professor L. Henkins remarks in comment 1 to §421 that modern concepts of jurisdiction to adjudicate under international law are similar to those developed under the due process clause of the United States Constitution; whereas, professor F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 4 (1990, Clarendon Press, Oxford) [hereinafter MANN] claims that the "Due Process" as understood in modern American law cannot provide firm guidance to the doctrine of international civil jurisdiction. "The international environment has not followed the sensational changes" US Supreme Court made in 1945 in *International Shoe v. State of Washington*, 326 U.S. 310 (US 1945). [In tort cases U.S. courts uses the "Calder-effect-test", *Calder v. Jones*, 465 U.S. 784, 788, FN6 (U.S. 1984)]. F.A. Mann firmly rejects a U.S. theory by which "under international law the jurisdiction of a State depends on the interest that State, in view of its nature and purposes, may reasonably have in exercising the particular jurisdiction asserted," stated in HENKIN, PUGH, SCHACHTER AND SMIT, INTERNATIONAL LAW, CASES AND MATERIALS 421 (1980). What is relevant, it is not the subjective or political interest, but the objective test of the closeness of connection, of a sufficiently weighty point of contact between the facts and their legal assessment, MANN 15.

[184] La Loi Toubon (No. 94-665 of 4 August 1994) in French and with an English translation at <http://www.globalvis.com-toubon.html> (visited August 2003).

[185] See footnote 86.

[186] Restatement Tort (Second) §577A (1).

can only file a libel suit once in a certain state on basis of a particular edition of a book, periodical or newspaper. Thus, to this extent a plaintiff has had to sum up his total claim in that state with respect to that published edition.

However, as for the Internet there are however new aspects. There can be no doubt that a person making a website on which he makes a defamatory statement about another person with all reasonableness should expect to be sued at the place of the defamed persons location.

The question is whether it is reasonable to let the provider of private person's access to the Internet or the host of a website to be liable together with the writer of the libel. Telephone companies have not been made liable for slander made over phone lines that could be recorded and thus are stored – just as a website can be downloaded.

As for such providers it seems reasonable to let them "go free" and regard them as only "pipelines," thus immunize them as the U.S. has done with the DCA §230.[187] The argument at first sight against such a regime is that with the Internet it has become much more difficult for the defamed person to find the author/publisher of the website. However, this is no more a detective problem than it is to find the editor of a newspaper with a defamatory statement issued in a small town on the other side of the globe. There is no reason to let the "pipeline" suddenly become liable together with the author/website publisher just because it is much easier to go for the "pipeline" company.

Thus, as far as the provider is not engaged in the publication is seems fair to immunize the provider – including providers offering chat-room and bulletin boards. However, it is questionable if it is reasonable to let providers such as AOL and Yahoo that either by subcontract (Drudge Report – *Blumenthal*-case[188]) or directly issues news to go free, as is the situation in the US.

It seems fair to let the publisher of a website only to be sued once for a particular libel. A publisher of a book or newspaper cannot recall the sold issues containing the libel, but once he has paid compensation for the libel to the defamed person, the publisher is immunized for further claims from the plaintiff as for that edition. However, this immunity is only valid for the nation where the court was sitting. Thus, the publisher could still risk being

[187] 47 U.S.C. 230 (effective October 21, 1998).
[188] *Sidney Blumenthal v. Matt Drudge*, 992 F.Supp. 44 (D.D.C. 1998).

sued by the same plaintiff in other nations where he chooses to sell the edition.

Much point in direction of regarding the Internet as "one nation" in the present discussion as the website can only be issued once, cannot be divided into selected nations, and it is fairly easy, cheaply and nearly instantly for the defamed person to react online defending himself.

Thus, courts ought to use a single publication rule to Internet defamation cases, and thus:

- First, determine if the Internet is an aggregate communication similar to newspapers, radio, television, and motion pictures.
- Next, the court must decide when the statute of limitations begins to run.
- The court must determine whether the continued appearance of the material on the Internet constitutes a republication of the defamatory material, a circumstance that exempts the material from the protection of the single publication rule.
- Finally, the courts must agree to a principle that prevents forum shopping, thus decide where the tort is regarded as being done, which is determining for what nations tort law should be used – or decide to make a universal online-libel rule.

It this regard it might be reasonable to make a distinction as to whether the libel is available through the Internet for the general public or only for a selected group of people. Such a split is demonstrated by U.S. case law in *Firth*[189] respectively the *Swafford*.[190] The rationale is that the single publication rule is appropriate for Internet defamation cases where the information is contained in an aggregate publication accessible to the public, as application of the multiple publication rule to Internet materials that are widely available would result in the very problems that the single publication rule exactly aims to resolve - namely to force plaintiffs to merge every single claim into one lawsuit once an for all, or loose a claim. On the other hand where only people with access to a certain database, the publisher has the possibility of control of who can read the content on the network and thus prevent access to people

[189] See footnote 112.
[190] See footnote 106.

that might think a statement as being a libel.

Against such a regime can be argued that the single publication rule has never been extended to rebroadcast television, radio. The rationale behind this is that each subsequent broadcast has renewed impact and "is intended to and does reach a new audience."[191] An Internet communication can be regarded as similar to a television or radio broadcast, since it to a certain extent has renewed impact with each viewing, and Internet-information is intended to and does reach a new audience every minute of every day.

However, the Internet-content might not be renewed, and television news can be taped by consumers and viewed for the first time a later time than the broadcast itself. Thus, even for broadcast there is no certainty that all viewers will see/hear the same libel at the same time – just as viewers might look at the same website at a different time. At the same time can be argued, that when something is uploaded to the Internet, the content is published once and for all to everybody on Earth, and the publisher cannot decide when the different readers will read the uploaded edition. Thus, there is no "second copy" with purpose to hit a new group of people as required in *Kanarek*[192] and the *Firth* Appeal[193] cases. The latter case further rejected that each "hit" to a certain website-address should be regarded a new publication retriggering the statute of limitations.

As for U.S. case law, should be remembered that even for the Single Publication Rule the date of "publication" varies widely from state to state.

For the Internet, there can be no doubt that the determining factor must be the time when the libelous article is made available to a third person, that is, from the time the article is uploaded to the computer network.[194] The limitations period should as held by the Fifth Appeal court run from the first posting of the defamatory matter upon an Internet website, not from the time of the reading by a third-party.[195] There seems to be equal good argument for and against whether the move of a libel article to another URL address should

[191] Comment D to Restatement Tort (Second) §577A.
[192] See footnote 103.
[193] See footnote 112.
[194] See footnote 119.
[195] See footnote 112.

be regarded as a republishing.[196] It will be difficult for a defamed person to find out whether the particular viewed website is the original; and a "move" will always be either "a copy and paste" of the website's source code or a new upload of the file containing the libelous article. Noteworthy is that the first *Firth* case held the single publication rule applies to Internet publications and modifications of unrelated portions of a website do not constitute republication. The second lower Firth case held otherwise.[197]

As for the defamed person, the Single Publication Rule has at least one large advantage. It allows plaintiffs to apply the longest limitations period available to all of their damages.

However, as the above listing shows not all U.S. states have adopted the Single Publication Rule and there are in the United States therefore "holes" where each of several communications to a third person by the same defamer is still regarded as a separate publication.

As online newspapers are published in every state and nation in the world – except where special access-features are required – the special U.S. Single Publication Rule has no great impact for online newspapers as a defamed plaintiff has the ability to choose a state or nation where the rule is not adopted.

Further, as for online newspapers it should be pointed out that its articles often are 20% to 70% shorter than print news stories [198] - only a few online editions contain the entire content of the print edition - and often they contain information never available in the paper-version.[199] - The online newspapers

[196] See footnote 118.

[197] *Firth* at 247, see footnote 112. Lower case, *Firth v. State of New York*, 12 A.D.3d 907, 785 N.Y.2d 755 (N.Y.AD.3 Dept., 18 November 2004) *leave to appeal denied* by 4 N.Y.3d 709, 830 N.E.2d 1145, 797 N.Y.S.2d 816 (N.Y. May 2005).

[198] J.E. Hyde, *Decoding the codes: A content analysis of the news coverage of genetic cloning by three online news sites and three national daily newspapers*, 1996 though 1998. (Doctoral dissertation, New York University, April 2001) DAI-A 61/10, page 3814.

[199] Jack Lovelace & Kirk Hallahan, *Pricing, content and Identity Issues at U.S. Online Newspapers – A Survey of Editors*, August 2003, page 5 at <http://lamar.colostate.edu/~pr/onlinelovelace040103.doc> (visited October 9, 2004) and Kevin Fagan, *Battling to Preserve Remnants of History*, SAN FRANCISCO CHRONICLE, 2 November 2000, A17.

often have special features other than paper-versions, for example the ability to add audio, video, and animation to news stories and other content, including advertisements. In addition, the ability to engage readers in two-way communication has been one of the distinguishing features of online publishing.[200]

This gives rise to the question of whether the online newspaper at all can be regarded as a copy of the paper version and thus be embraced by the Single Publication Rule with respect to paper versions. At the same time it should also be remembered that online news-articles often are continuously updated, which shut out the use of the Single Publication Rule as this rule only deal with claims related to a single edition and supplemental supply copies hereof in time made close to the first print.

As for libel cases related to Internet content, there seem on one hand to be good reason for using a retraction rule, as it is fairly easy and quick for a publisher to correct or clarify libelous content. However, while it might be a requirement of the publisher to retract his content, this might not be sufficient as a copy of the content could be stored on a proxy server that the publisher does not know about. But, this situation is no different from the brick and mortar world where the libelous newspaper will still be "stored" at the customers. The advantage in Cyberspace would be that the original content-edition could be corrected, whereas in the brick and mortar world a correction - at least for newspapers - will have to be in a successive edition.[201] The same main arguments for the present retraction statutes can be made for Cyberspace see above section 5.5.1.3. To the Cyberspace issue should be added that a correction of the wrongful edition should not be regarded as a new edition as this would begin a new single publication period.

[200] Jennifer Greer & Donica Mensing, *Evolution on Online Newspapers: A longitudinal content analysis*, 1997-2003, October 1, 2003, at < http://list.msu.edu/cgi-bin/wa?A2=ind0310a&L=aejmc&D=0&P=1228> (visited September 2004).

[201] This might not be necessary for newspapers delivered by electronic ink, which allows updating. E-Ink is a "smart" material that changes its image when exposed to an electric field. COMPAINE *supra* note 160 at 475 (Chapter 7 "The Online Information Industry").

5.8. Final Remarks

As not even the states in the U.S. can agree to a unified Single Publication Rule – or a mandatory federal statute – then it is hard be believe that such a rule will immediately become so broadly internationally accepted that it can become accepted as custom international law. Thus at present, the "custom" in international law – and thus on international public computer networks – is the "multiple publication rule," which state of things online newspapers and other online publishers have to accept and base their business upon.

Neither can a "retraction rule" be said to be custom in public international law.

However, that does not mean that the basis requirement of reasonableness in public international law does not point in the direction of a "single publication rule" on international computer networks – or maybe an online "retraction rule" for publishers could achieve the same goal!

Furthermore, one can hope the reasoning of the Appeal Court of Ontario in *Bangoura*[202] will be followed by other courts in the world. It seems more than reasonable that a court rejects a case on lack of jurisdiction, if the defendant was not a resident or national in the forum of the court at time the defamatory content (first) was published. This will prevent plaintiff's forum shopping as in the English *Don King* and *Schwarzenegger* cases.[203] See also final remark in section 5.6.3.

[202] See footnote 125.
[203] See above footnotes 145 and 148.

CHAPTER 6

An international dispute on the Internet - Californian Yahoo! Inc. versus France

By Henrik Spang-Hanssen[1]

6.1. Introduction

The following deal with a dispute that involves public international law and that could not have happened but for the existence of public international computer networks.

This case was between the Silicon Valley firm Yahoo! Inc. [hereinafter Yahoo] against two French organizations [hereinafter LICRA]. The object of the latter is the fight against racism and persecution of the Jews in France.2 The U.S. Federal Court of Appeals for the Ninth Circuit held in on August 23, 20043 that there did not exist jurisdiction for the U.S. District Court in

[1] Partly translation of Henrik Spang-Hanssen, *Californiske Yahoo! Inc. contra Frankrig: en international tvist på Internettet*, LOV & DATA page 18-22, 4/2004; *Opdatering i sagen Yahoo! Inc. mod LICRA*, LOV & DATA page 7, 2/2005; and *Afslutning på Yahoo-sagen*, LOV & DATA page 33-35, 1/2006 [Law and Data Journal] (Published in Scandinavia, ISSN 0800-7853).

[2] La Ligue contre le Racisme et L'Antisemitisme and L'Union des Etudiants Juifs de France.

[3] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 379 F.3d 1120 (9th Cir. 23 august 2004 – No. 01-17424) and at <http://caselaw.lp.findlaw.com/data2/circs/9th/0117424p.pdf> (visited September 2004). The parties briefs are found in Westlaw under 2002 WL 32302222, 2002 WL 32302223, , 2002 WL 32302225, and a Amici Brief from the Center for Democracy

Santa Clara (including Silicon Valley).[4] Yahoo asked the same Appeal Court to rehear the case en banc,[5] which was granted in February 2005.[6] Rehearing was held on March 24, 2005 and a decision was issued in January 2006, see below. Yahoo has abstained from asking the U.S. Supreme Court to deal with the case.[7] It has been supported by several organizations.[8]

6.2. Facts in the Civil Case

The facts of the case are briefly,[9] that LICRA in France on November 20 2000 achieved a court order against Yahoo France and its parent company, American Yahoo! Inc. The two defendants were ordered to secure that Frenchmen could not on Yahoo related websites see anything relating to Nazism.[10] Pursuant to the French judge, the French corporation has fulfilled the order, whereas the American parent company has argued (1) it is impossible in practice to fulfill its obligation in the order, and (2) that the order is conflicting with amongst others the First Amendment of the U.S. Constitu-

and Technology, American Civil Liberties Union, Electronic Frontier Foundation, Human Rights Watch et. al. [hereinafter "Amici Curiae"] under 2002 WL 32302224.

[4] United States District Court for the Northern District of California – and with that - presumably any court in the U.S.

[5] "Rehearing en banc" requires approval of the judges in the Ninth Circuit, Federal Rules of Appellate Procedure Rule 40. In the 9th Circuit a "full" panel of judges consists of the President of the Court and ten other judges, Local Circuit Rules 35-3.

[6] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme,* 399 F.3d 1010 (9th Cir 2005).

[7] The U.S. Supreme Court determines on its own (with few exceptions) what cases it wished to decide, Supreme Court Rule 13. The time-limit is ninety days after a lower court has decided the case.

[8] Amici Curiae Brief of September 13 2004 at <http://www.cdt.org/jurisdiction/20040921amici.pdf> (visited September 26, 2004).

[9] The facts in the case are detailed laid out at pages 184-188 and 483-503 in HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION (DJØF Publishing, 2004 –ISBN 87-574-0890-1) [hereinafter SPANG-HANSSEN].

[10] The French decisions of May 22 2000 and November 22 2000 are exhibited (and in an English translation) to Yahoo! Inc.'s writ to the court in California, at <http://www.cdt.org/speech/international/ 001221yahoocomplaint.pdf> (visited August 7, 2000).

tion and several international human rights instruments.

Furthermore, the French court order imposed on Yahoo! Inc. daily fines of 100.000 Franc – that as of December 31 2005 has accumulated to circa 320 million dollars - which fines for any corporation quickly can become a matter of vital importance or even make it consider filing for bankruptcy. Thus, Yahoo asked in 2000 its local court in California to decide it would neither execute the French order, if LICRA later should ask for enforcement of the French decision.

LICRA has in the American case argued that American courts cannot deal with the case, since the French parties has no connection to or property in the U.S.

6.3. Facts in the French Criminal Case

Parallel with the civil case filed by LICRA in France, the French Prosecutor and two organizations filed in October 2001 a criminal case at the Criminal Court in Paris[11] against the of that time being CEO of the American Yahoo!. In the criminal case, Timothy Koogle was accused of (1) justifying a crime against humanity and (2) the exhibition of a uniform, insignia or emblem of a person guilty of crimes against humanity.[12] The first charge has a maximum fine of 45,700 € and five years' imprisonment; the second a fine of 1,500 €.

On February 26, 2002, the Criminal Court in Paris rejected defendant's argument that the court did not have jurisdiction over acts done in the U.S. by an American citizens and an American corporation.[13] The Paris Criminal court disagreed with the U.S. federal district court's ruling of November 7 2001 that Yahoo! was under no obligation to comply with French laws on its

[11] *Procureur de La Republique, Association Amicale des Déportés d'Auschwitz et de S Camps de Haute Silesie and M.R.A.P. Mouvement contre le racisme et Pour L'amitié entre les Peuples v. Société Yahoo! Inc et Timothy Koogle* (Tribunal de Grande Instance de Paris, 17eme Chambre - No d'affaire: 0104305259) .

[12] It is illegal under French law to exhibit or sell objects with racist overtones, and Yahoo's French site offered no Nazi auctions.

[13] Tribunal de Grande Instance de Paris, Jugement du: 26 février 2002 (17eme Chambre - Chambre de la Presse, No d'affaire: 0104385259), <http://www.juriscom.net/documents/tgiparis20020226.pdf> (visited April 25 2002).

American websites, and noted that it had the right to adjudicate the charges, as the site was accessible in France. The French criminal court ruled, that French justice remains free to adopt the principles of international judicial competence that it has to sanction certain infraction committed entirely or partly abroad and that are likely to harm national interests. Thus, the French court ruled that it was competent to hear the case against the defendants.

In a court meeting on January 7 2003, prosecutor David Peyron called for no punishment to be levied in case of a conviction. He noted that the second charge had been dropped under a nationwide amnesty decreed by President Jacques Chirac after his re-election in 2002.[14]

In a judgment of February 11, 2003, the French criminal court in Paris acquitted the defendants as the court found neither Timothy Koogle nor Yahoo! did condone or praise Nazism and that they had not shed favorable light on the policies of Adolf Hitler by selling objects from the Third Reich. The Criminal court in Paris ruled that neither charge against Yahoo! or Koogle had been proved. Under French laws, the court said, "justifying war crimes [or] crimes against humanity" means "glorifying, praising, or at least presenting the crimes in question favorable." According to the court, the activities of Yahoo! did not match this definition and held that Yahoo never tried to justify war crimes or crimes against humanity.[15] The prosecutor decided not to appeal the judgment. However, the two other plaintiffs appealed the judg-

[14] AFP, *French prosecutor argues for no sentence for former Yahoo! boss on trial*, YAHOO! NEWS SINGAPORE, January 8, 2003, at <http://sg.news.yahoo.com/030107/1/36ajx.html (visited January 8, 2003), Reuters, *French courts aquits ex-Yahoo chief over Nazi sites*, LYCOSNEWS, February 11, 2003 at <http://news.lycosasia.com /sgen/> NEW YORK TIMES, February 11, 2003, <http://www.nytimes.com/reuters /technology/tech-crime-france-yahoo.html> & NEWS.COM, February 11, 2003 at <http://news.com.com/2100-1023-984148.html> (all visited 18 February 2003), Out-Law.com, *French court acquits Yahoo! of criminal charges for Nazi sales*, OUT-LAW.COM, February 12, 2003 at <http://www.out-law.com/php/page.php?page_id= frenchcourtacquits104505511&area=news> (visited February 19, 2003) & Center for Democracy & Technology, *French court rules in favor of Yahoo in Internet free speech case*, cdt.org at <http://www.cdt.org/jurisdiction> (visited October 2003).

[15] Tribunal de Grande Instance de Paris, 11 février 2003 (17eme Chambre - Chambre de la Presse, No d'affaire: 0104385259 -).

ment, but only over Koogle as French law did not permit the case against Yahoo! to be appealed.

On March 17 2004, the Appeal Court of Paris[16] affirmed the decision of February 22 2002 from the Criminal Court of Paris, pursuant to which the court has jurisdiction over Koogle, because American Yahoo's auction-websites contained sales of Nazi-effects, which could be seen by Frenchmen, and that the French Criminal Code could be used.

Koogle was acquitted by the Court of Appeals in Paris on April 6, 2005.[17]

6.4. The French Civil Case

In the French civil case, LICRA wanted Yahoo to remove websites that the organizations found offensive and violating French law, which prohibits promotion of Nazism, persecution of the Jews and sale of Nazi-effects or objects.

In this connection should be pointed out that in France exists – opposite other countries – a special law, the Toubon law,[18] which requires that web-sites related or aimed at French Territories must be formulated in French. This requirement (as well as other French law) is observed and complied with by Yahoo's French subsidiary, as nearly almost of its websites uses French

[16] *Le Ministère Public, Association Amicale des Déportés d'Auschwitz et de S Camps de Haute Silesie and M.R.A.P. Mouvement contre le racisme et Pour L'amitié entre les Peuples v. Société Yahoo! Inc et Timothy Koogle* (Cour D'Appel de Paris - 11ème Chambre, section A – Dossier No 03/01520). Lionel Thoumyre , *La Cour d'appel de Paris se déclare compétente pour examiner la responsabilité de l'ex-PDG de Yahoo! Inc*., JURISCOM.NET March 17 2004, at <http://www.juriscom.net/actu/visu.php?ID=477> (visited August 28 2004); *Appeal court to try former Yahoo! boss in Nazi memorabilia case,* AFP, March 17, 2004 at <http://uk.news.yahoo.com/040317/eotuk.html>.

[17] *French Appeals court says Yahoo not liable for Nazi gear auctions*, SILICON VALLEY.COM, April 6 2005 at <www.siliconvalley.com/mldsiliconvalley/news/editorial/11326488> and *Ex-Yahoo CEO's Nazi auction acquittal upheld in France*, OUT-LAW.COM, April 7, 2005 (visited April 7, 2005).

[18] La Loi Toubon (No. 94-665 of August 4 1994), in French and with a English translation at <http://www.globalvis.com-toubon.html> (visited August 2003).

words. Yahoo's parent corporation in California is aimed at the U.S., and its websites are therefore formulated in English. However, American Yahoo seems not in the court to have argued, that its websites only are using English words and therefore cannot be aimed at Frenchmen or French Territories.

Californian Yahoo offers for free amongst others to its customers to constructs websites at <www.geocities.com> and at Yahoo's auctions-site to self-type information and upload pictures of effects the customers want to sell. Thus, these sites are in reality formulated by the users themselves, as Yahoo only removes content in an insignificance number of cases. Yahoo does in reality not make any censorship, monitoring or supervision of its customers' use of the offered services, which to a certain extent would be in violation with the First Amendment of the U.S. Constitution.

Yahoo argued for the French court that it was technically impossible to sort out or filter objectionable websites. This prompted the French judge to appoint a panel of three computer-experts, consisting of French state-employed François Wallon, British professor Ben Laurie, and one of the fathers of the Internet-protocol, American Vinton Cerf. The French judge used the report from the experts, as basis for the order of November 20, 2000.

However, the value of the report of the experts should be considered. The report is written in French, a language that at least American Vinton Cerf does not speak or read. There exists no English translation. The British expert was prevented from participate in a meeting between the parties, the experts and the judge. The judge did not permit the meeting to be rescheduled. Vinton Cerf wanted to make further inquiries before the report was issued, which request was not granted by the French judge. American Vinton Cerf has vigorous and powerfully criticized the decision of the French court as he finds the decision is based on an erroneous perception of the technicality of the Internet. The British expert has forthright apologized for the report and stated that is only has a limited value, because the French judge only allowed a very limited number of questions answered by the experts. This latter prevented the expert-report to fulfill its purpose and give a proper description of the possibilities – or lack of such – to control content on the Internet.[19]

An expert on computer networks has stated, that the present technical pos-

[19] On this, see further SPANG-HANSSEN *supra* note 9, at 186.

sibilities to locate and relate certain content on the Internet to a certain local-community only works to such a degree that is acceptable for business use, but far from the demands of certainty that a court evidently must require to let the computer-technique be the decisive for purposeful behavior and conduct, that is in this context, the question of jurisdiction.[20]

Furthermore should be remarked, that the French order pursuant to its own contents not is a final and definitive decision, as the French (state-employed) expert (not yet) has given a presumed and required report to the French judge on whether Yahoo has complied with the order of the court, and partly as the court has reserved a right to change the resolution of fines.

LICRA has until now not declared whether it will initiate enforcement in the U.S. of the French order.[21]

6.5. The American Civil Case

Initially should be pointed out, that the U.S. Supreme Court in 1945 decided that the decisive for whether there exists jurisdiction for American courts to deal with a case over a non-resident is that there exists "minimum contacts" between the defendant and the forum state, and that exercise of jurisdiction is pursuant to "fair play and substantial justice".[22] The State of California has in

[20] Former Bell Labs researcher Bill Cheswick, Lumeta Corp., to Stefanie Olsen, *Geographic tracking raises opportunities, fears*, CNET News.com, November 8 2000, at <http://news.com.com/2100-1023_3-248274.html> (visited October 14 2003). On the possibilities of filters, see SPANG-HANSSEN *supra* note 9, Chapters 11 and 31.2. On the possibilities of geographic locationing, see SPANG-HANSSEN *supra* note 9, section 31.2.1.

[21] During the re-hearing on March 24 2005 the attorney for LICRA stated that his clients was of the opinion that Yahoo had complied with the order, and that they would not enforce the French decision in the U.S. and thus collect the fines, unless Yahoo returned to previous practices.

[22] Further on these conditions, see HENRIK SPANG-HANSSEN, CYBERSPACE JURISDICTION IN THE U.S.: THE INTERNATIONAL DIMENSION OF DUE PROCESS 27-36 (Complex 5/2001, Published by the Norwegian Center for Computers and Law, Oslo University 2001 - ISBN 82-7226-046-8), also free downloading from <www.geocities.com/hssph>; and KIM ØSTERGAARD: ELEKTRONISK HANDEL OG INTERNATIONAL PROCES- OG PRIVATRET 131-160 (DJØF Publishing, Copenhagen 2003). American courts sharply distinct be-

section 410.10 of its Code of Civil Procedure decided that its rules on personal jurisdiction shall go to the maximal extent allowed by the U.S. Federal Constitution, thus, the requirement set forth by the U.S. Supreme Court in 1945.[23]

On June 7, 2001, the Federal District Court in Santa Clara held it had personal jurisdiction over LICRA, since the requirement made by the Supreme Court was fulfilled.[24] At a later decision of November 7, 2001 the same district court decided that (1) there existed an actual controversy, (2) that the French order constituted a real and immediate treat against Yahoo's constitutional rights, (3) that the court would not enforce the French order in the United States.[25] The court pointed out that LICRA had send a "cease-and-desist letter"[26] to Yahoo in California, that LICRA utilized the United States Marshal's Office to serve Yahoo! with process in California about the French lawsuit, and that LICRA tried to force Yahoo to do acts on its computers placed in California.

The Ninth Circuit decided in a 2-1 decision of August 23 2004[27] that LICRA was not embraced by existing American jurisdiction rules, wherefore it could not be sued in the United States. The court pointed out that the decisive for the jurisdictional question was whether LICRA's acts was specially targeting or aimed against Yahoo! in California.

The majority did not find that LICRA fulfilled the standard, which the Ninth Circuit had outlined in its previous case, *Bancroft & Masters*,[28] after which the decisive is, that defendant's act is expressly aiming a specific person and that the conduct is not unreasonable. LICRA had a legal right to take

tween questions and facts related to the question of (personal) jurisdiction, and questions and facts related to the "subject matter" of the case.

[23] On American practice on jurisdiction in relation to online-business, see this book Chapter 4.

[24] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 145 F.Supp.2d 1168 (N.D.Cal. Jun 07, 2001).

[25] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 169 F.Supp.2d 1181 (N.D.Cal. Nov 07, 2001) (NO. C-00-21275 JF).

[26] A letter requesting a party to stop doing something or risk being suit in court.

[27] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 379 F.3d 1120, 1126 (9th Cir. Aug 2004).

[28] *Bancroft & Masters, Inc. v. Augusta Nat'l Inc.*, 223 F.3d 1082 (9 Cir. 2000) .

action in France against Yahoo for violation of French law, and Yahoo! had to wait for the foreign litigants to come to the United States to enforce the French judgment before its claim could be heard by a U.S. court. Yahoo did not make any allegation that could lead a court to conclude that there was anything wrongful in the organizations' conduct. The majority further remarked, that Californian Yahoo could not expect both to benefit from the fact that its website content may be viewed around the world and to be shielded from the resulting costs - one of which is that Yahoo! violates the speech laws of another nation.

The Third judge pointed out in his dissent, which has the double length as the courts decision, that it is not necessary for the jurisdictional question that there exists an "express aiming" against Yahoo. He held that LICRA's whole conduct was sufficient to allow an American court to deal with the claims made by Yahoo. In this connection, he noticed the latent treat that rested upon Yahoo to pay significant and daily accruing fines if Yahoo! refused to so comply. It was in his opinion immaterial whether LICRA and UEJF had yet to enforce the monetary implications of Yahoo!'s refusal to acquiesce in the French court order.[29]

Because the Ninth Circuit decided that the District Court did not have personal jurisdiction over the French parties, the Circuit did not review whether Yahoo!''s action for declaratory relief was ripe for adjudication or whether the District Court properly refused to abstain from hearing this case.[30]

In February 2005, the Ninth Circuit decided to rehear the case en banc.[31]

During the rehearing on March 24, 2005 the counsel for Yahoo! informed that not all Nazi content has been removed from for example Yahoo! auctions sites from which still is for example made sales of stamps and coins related to the Nazi period.

On January 12, 2006, the Ninth Circuit decided the case[32] and per curiam reversed and remanded the decision of November 7, 2001 from the District

[29] 379 F.3d 1120, 1127.
[30] 379 F.3d 1120, 1127.
[31] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 399 F.3d 1010 (9th Cir. Feb 10, 2005) (NO. 01-17424).
[32] *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199 (9th Cir. Jan. 12, 2006).

Court [33] with instructions to dismiss without prejudice.[34]

6.6. The Ninth Circuit's decision of January 2006

The eleven judges have written a decision of 99 pages that clearly shows the judges have disagreed to a large extent about which decision should be made. The decision is per curiam and only achieved by counting the votes from five different opinions.[35]

Under facts the court noted that Yahoo had not pursued all its possibilities of appeal in France, and that the French parties had not been willing to ask the French court to vacate or recall its orders.[36]

The Appeal Court remarked further, that after conducting its own Internet research on yahoo.com, the District court found that even after Yahoo had made some policy change, Yahoo! "appear[s] not to have fully complied with the orders with respect to its auction site".[37]

A group of eight judges initially pointed out that the only bases for personal jurisdiction over LICRA and UEJF in the district court was if there existed facts showing the foreign defendants had minimum contact with a court in the U.S. and it was reasonable to deal with the case. The French organizations had no physical contacts or employees in the U.S. The majority held that sending a cease and desist letter to Yahoo! at its headquarters in Santa Clara, California, was in and of itself not sufficient to establish personal jurisdiction over the sender of the letter.[38] It further held that the serving process on Yahoo! in Santa Clara to commence the French suit could not by themselves justify the exercise of personal jurisdiction over a foreign litigant in a United States court.[39] The most important factors for finding personal jurisdiction over the two French organizations was that they had obtained two interim orders from the French court directing Yahoo! to take

[33] 169 F.Supp.2d 1181.
[34] 433 F.3d 1199, 1224.
[35] 433 F.3d 1199, 1224.
[36] 433 F.3d 1199, 1204.
[37] 433 F.3d 1199, 1205 with reference to 169 F.Supp.2d 1181, 1185 (N.C.Cal. Nov. 2001).
[38] 433 F.3d 1199, 1208.
[39] 433 F.3d 1199, 1209.

actions in California, on threat of a substantial penalty.[40] These judges believed that the French organizations had deliberately target California, wherefore the requirements for exercising personal jurisdiction was fulfilled. In this connection the majority took the opportunity to "clarify our law and to state that the "brunt" of the harm need not be suffered in the forum state. If a jurisdictionally sufficient amount of harm is suffered in the forum state, it does not matter that even more harm might have been suffered in another state."[41]

The other three judges on the bench held that the district court's decision should be reversed and the case dismissed.[42] They did not believe that lack of ripeness[43] was the proper ground to dismiss Yahoo!'s suit. Instead, they believed that the District Court had not properly exercised personal jurisdiction over the defendants and also should have abstained from deciding Yahoo!'s claims.[44]

Of the group of eight judges, five further held that the case was ripe and should be decided,[45] because the issue before the court was whether a United States Internet service provider, whose published content has been restricted by a foreign court injunction, may look to the United States federal courts to determine the enforceability of those restrictions under the United States Constitution's First Amendment. The French injunctive orders - backed by substantial, retroactive monetary penalties for noncompliance - required Yahoo! to block access from French territory to Nazi-related material on its website. Some prohibited content was readily identifiable, such as Nazi artifacts or copies of Mein Kampf. Much, however, was not. In traditional First

[40] 433 F.3d 1199, 1209.
[41] 433 F.3d 1199, 1207.
[42] 433 F.3d 1199, 1224.
[43] Ripeness: (1) The circumstance existing when a case has reached, but has not passed, the point when the facts have developed sufficiently to permit an intelligent and useful decision to be made. (2) The requirement that this circumstance must exist before a court will decide a controversy. The opposite of the Mootness Doctrine: The principle that American courts will not decide cases in which there is no longer any actual controversy (Black's Law Dictionary 8th ed. 2004).
[44] Pursuant to Federal Procedure Rule 12(b)(2) or 12(b)(6). Text as of December 1st, 2005 at <http://judiciary.house.gov/media/pdfs/printers/109th/civil2005.pdf> (visited January 2006).
[45] 433 F.3d 1199, 1233-53.

Amendment terms, this injunctive mandate was a prior restraint on what Yahoo! may post (or control access to) on its U.S.-located server - imposed under principles of French law and in such facially vague and overbroad terms that the court American did not know whether further restrictions on access by French, and possibly American, users were required to comply with the French orders.[46]

These judges found it unreasonable to require Yahoo to appeal the French order to a French court, which does not recognize the constitutional free speech in the U.S. First Amendment. Furthermore, these judges would not allow a foreign court to decide whether the guarantee of freedom of speech protected Yahoo! - and, derivatively, at least its users in the United States - against some or all of the restraints the French defendants had deliberately imposed upon it within the United States. They noted that "prior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights."[47]

This group of judges felt the other judges in the bench denied Yahoo! the only forum in which it could free itself of a facially unconstitutional injunction. Moreover, in doing so the majority created a new and troubling precedent for U.S.-based Internet service providers who may be confronted with foreign court orders that require them to police the content accessible to Internet users from another country.[48]

From the group of eight judges, three held the case should be dismissed, because they were uncertain about whether, or in what form, a First Amendment question might be presented to the court.[49] Further, they found it was exceedingly unlikely that any court in California - or indeed elsewhere in the United States - would enforce the French order since it imposed a monetary penalty against Yahoo! and California law does not authorize enforcement of foreign "fines or other penalties."[50] Furthermore, these judges interpretated (translated from French) and emphasized the French court's interim orders did not by their terms require Yahoo! to restrict access by Internet users in the

[46] 433 F.3d 1199, 1234, 1252-53.
[47] 433 F.3d 1199, 1235, 1252-53.
[48] 433 F.3d 1199, 1235, 1253.
[49] 433 F.3d 1199, 1217, 1221.
[50] 433 F.3d 1199, 1218, 1221.

United States. In their interpretation, the orders only required Yahoo! to restrict access by users located in France.[51] Finally, these judges held that Yahoo! had presented the case in such a way that the record was "inadequate, incomplete or unclear". The judges pointed out that First Amendment issues arising out of international Internet use are new, important and difficult.[52]

The result of the case is, that there exists personal jurisdiction over the two French organizations in the district court, but that the subject matter is not ripe for consideration, wherefore the appeal court has instructed the district court to dismiss without prejudice.[53]

6.7 Comments to the decision

By the decision of January 12, 2006 the lawsuit must be regarded to be finished, since the uncertainties mentioned in the appeal court decision presumably rule out that the judges in the U.S. Supreme Court will accept the case (at the present time).

One can regret that this case has not been prepared better of the involved council of Yahoo!. In an international dispute like the one at issue, it does not seem reasonable and appropriate that there only participate attorneys from the same Nation of the court. This situation preclude that the parties in the court has the possibility to answer questions from the bench about the law in the other involved Nation. In the meeting in the American appeal court, the participating (American) attorneys could not answer questions about French law, enforcement and so on.

In addition, as a European one is astounded that the American attorneys and/or the American courts did not required authorized translations of the French orders and of the report from the French court's experts. This would without doubt have been a fundamental demand from European judges. In the present case several of the appeal court judges have made own interpretations and translations of French phrases and terms, and these judge-perceptions have to a large degree decided the case in an unacceptable way, because some

[51] 433 F.3d 1199, 1221.
[52] 433 F.3d 1199, 1223.
[53] 433 F.3d 1199, 1224.

of the understandings are outright wrong or incorrect. The translations the court has used was enclosed in Yahoo!'s brief.[54]

Also, it is for example astonishing that the judges have used a translation[55] of a statute in the French Penal Code,[56] which has been found on a website made by an American lawyer, which is a professor in international business law at the University of Riga, Latvia.[57] The translation is erroneous and uses for example the term "crime" in stead of "minor defense" [in French "contravention"] (without possibility of imprisonment), compare with a translation by a French speaking professor (who is also an authorized translator) on webpage <www.geocities.com/hssph/R645-1_Toman.pdf>.[58]

Some of the judges have assumed that Yahoo should initiate the work of a report (and blame Yahoo for not having delivered the report),[59] which also is a based on a wrongful translation of the French order of May 22, 2000, which a later order of November 20, 2000 make reference to. Correct translations can be found at <www.geocities.com/hssph/Order22May2000_EN_Toman.pdf> and <www.geocities.com/hssph/Order20Nov2000_EN_Toman.pdf>. The French judge made a direct order to the French expert, Mr. Wallon, to find out – after the end of a three month period – whether Yahoo had complied with the court's order.[60]

The same group of judges, confer footnote 1 in the decision, base their decision on the remark from the French parties' American attorney's personal opinion (or translation) of the content of the French order. However, pursuant

[54] Complaint in the American Case at <www.cdt.org/speech/international/001221yahoocomplaint.pdf> (visited August 2001).

[55] <http://www.lex2k.org/yahoo/art645.pdf> (visited January 2006).

[56] 433 F.3d 1199, 1219.

[57] <www.rgsl.edu.lv/index.php?part=masters&page=faculty_details#1> (visited January 2006).

[58] Where the French legal term "contravention" is explained. See also JOHN H MERRYMAN, THE CIVIL LAW TRADITION: EUROPE, LATIN AMERICA, AND EAST ASIA 547 (The Michie Company 1994 – ISBN 1-55834-180-3). The latter on page 550 has an overview of the structure of the French Court System.

[59] 433 F.3d 1199, 1216.

[60] <www.geocities.com/hssph/Order20Nov2000_EN_Toman.pdf>.

to an authorized translator is the attorney's – and thereby the judges' – opinion erroneous.

Many of the American judges base their decision on the content of the remarks (or analyze) of the French judge written before the actual issued order or text of the injunction. Thus, these judges over-interpretate the content of the real issued French order. This is necessary for the majority to reach their decision and reject the dissenting judges. These judges read into the French order that it only deals with the French territory in Europe, but not the French territories that for example the report of November 6, 2000 from the French court's experts in footnote 2 at page 39 considered with reference to their appointment in the French judge's decree of August 11 and September 18, 2000. The experts understand the French order of May 2000 as including all French territories.[61] If the American judges had used the experts' understanding, the opinion of the majority would collapse like a house of cards.[62]

There is nothing in the French order that imply the order in relation to American Yahoo! only can be interpretated to concern the Internet users localized in the French European territory.

Furthermore, the French order is far from as explicit in its wording as the majority of the American judges interpretate it to be.

Apart from the decision's unlucky grounds and erroneous interpretations and translations, it seems fair that the majority of the judges held that there could be exercised personal jurisdiction over the two French organizations, which clearly had attempted to get Yahoo! in California to change its behav-

[61] France, French Polynesie, French New Caledonia etc., Rapport de Consultation at <http://www.law-links.ch/archiv00.html file rapportyahoo-6nov00.zip> (visited May 2003). In addition, many French people uses access-providers in Swiss and Belgium pursuant to Jean-Denis Gorin, Yahoo! Inc. expert witness and referred to at page 43 in the French Court's Rapport de Consultation.

[62] The majority admit itself: "If it were true that the French court's orders by their terms require Yahoo! to block access by users in the United States, this would be a different and much easier case. In that event, we would be inclined to agree with the dissent", 433 F.3d 1199, 1222. See also the minority's remark at 433 F.3d 1199, 1235: "The majority's thesis rests on the contention that the French "orders do not by their terms limit access by users outside France in any way" (Op. at 1216). But as the majority recognizes elsewhere in its opinion (Op. at 1216 - 1218), the crux of this case is not in the words of the order alone, but in their application".

ior. Besides this, the only fair alternatives seems to be the minorities opinion of deciding the subject matter as the district court did, or to dismiss the case, because the French order not is final and the possibilities for appeal in France has not been exhausted.

If the case had been presented properly of the council for Yahoo!, the case could have been the Internet's pendant to the S.S. Lotus case on the High Sea.[63] With present "result", Yahoo's shareholders still has to account with future loss in share price, if France decides to collect the – at present - fall due 320 million dollars.

6.8. Public international law aspects

As Amici Curiae[64] pointed out in its brief to the Ninth Circuit, the French court's order is an example of the sort of judgment, which foreign courts can expect will be presented for them with increasing frequency as Internet use expands throughout the world.

The French decision is reflecting the view that any country has a right to make rules on jurisdiction with a global reach when the Internet is involved.[65] Amici Curiae remarked that American courts overwhelmingly have rejected attempts to censor the public international computer networks and recognized the essential character of the Internet as a global medium. However, other nations have imposed controls on the Internet intended to silence disfavored expression originating within their borders and to keep out disfavored expression originating abroad. The Amici brief remarks that at least 59 different

[63] *S.S. Lotus* (France v. Turkey), 1927 P.C.I.J (Ser. A) No. 10. Also at <www.geocities.com/hssph/Lotus.doc>.

[64] Brief of Amici Curiae Center for Democracy and Technology, American Civil Liberties Union, et al., in Support of Appelee Yahoo! Inc. of May 6, 2002 to the 9th Circuit, 2002 WL 32302224.

[65] §246 of the Danish Civil Procedure Code allows broad global jurisdiction, see this book Chapter. Otherwise, §27 of the Norwegian Civil Procedure Code require a business has a physical location inside Norway and thus limits the possibility for global jurisdiction.

countries limit freedom of expression online.[66]

From the perspective of public international law, the Yahoo dispute also involving the French criminal case give reminders of the S.S. Lotus case before the Permanent Court of International Justice in 1927, where France argued, that Turkey did not have the right to punish a French seaman after a ship-collision on the (international) High Sea.[67] The international court held in a 6-6 decision with the Court-president's vote as decisive that Turkey had not violated public international law. There is no doubt that the court would not have allowed third-party-countries to deal with the case or punish the seaman.[68] In relation to human rights, Belgium has attempted to exercise exterritorial and global jurisdiction over an issue that had nothing to do with Belgium. The International Court of Justice in the Hague did not allow Belgium as a third-party to deal with the matter, as the offender was covered by diplomatic immunity rules under public international law.[69]

The perspective for example for businessmen like Yahoo's Koogle is dangerous and unsafe. If any country has a right to punish conduct or acts done on the Internet - even though it is legal in the businessman's own country - no businessman can any longer without risk of imprisonment travel to counties where the act is held illegal. If further the particular country is party to a

[66] Reporters Sans Frontieres, ENEMIES OF THE INTERNET 5 (2001) <http://www.rferl.org/nca/special/enemies.html> (visited January 22 2003); see also Douglas Sussman, *Censor dot Gov: the internet and press freedom* 2 (2000) <http://www.freedomhouse.org/pfs2000/sussman.htniJ>. An updated report includes Denmark – a country whose government praises the Internet and wants to be on a forefront information technology country, and with 80 % of the population having Internet access. THE INTERNET UNDER SURVEILLANCE - OBSTACLES TO THE FREE FLOW OF INFORMATION ONLINE, 2003 REPORT (Reporters Without Borders - ISBN 2-90-8830-88-4) <www.rsf.org/IMG/pdf /doc-22236.pfd> (visited September 2003). On censorship and firewalls, see Chapter 17 in SPANG-HANSSEN *supra* note 9.

[67] *S.S. Lotus* (France v. Turkey), 1927 P.C.I.J (Ser. A) No. 10. Also at <www.geocities.com/hssph/Lotus.doc>.

[68] The Permanent Court of International Justices observed that "the collision took place on the high seas [wherefore] the territorial jurisdiction of any State other than France and Turkey therefore does not enter into account", *id.* page 12.

[69] *Case concerning the Arrest Warrant of 11 April 2000* (Democratic Republic of the Congo v. Belgium) of 14 February 2002, 2002 ICJ 121, <http://www.icj-cij.org/icjwww/iCOBE/iCOBEframe.htm> and previous decision in 2000 I.C.J. 182.

treaty or agreement with others on compulsorily extradition, as is the case between the E.U. Member States, businessmen like Koogle can no longer travel to the 24 countries in the E.U. with certainty to be able to return to his own country after a business-meeting or holiday. In this connection should be remarked that pursuant to section 22.1.d of the Cybercrime Convention has it no significance or importance whether the "punishable" act was legal, if it is a violation in another country that is party to the convention.[70]

The trend seems to be in violation with public international law where the basis is the sovereignty of every country and its self-determination on its own citizens - with exception of the very specific issues where the public international society and thus public international law allows exercise of universal jurisdiction. Only in the latter case does any country have jurisdiction to deal with the specific (and limited) issue, such as piracy, slave trade. This latter is due to that there between the worlds nations has been a (overriding) agreement of regarding these specific issues as so blameworthy and reprehensible that the international society allows any state to react against them (so-called universal jurisdiction).

However, as for the Yahoo dispute, the fact is that Yahoo offers services (like a phone company) that gives the customers the full power, discretion and determinations of how and what information is going to be uploaded about the customer's effects to be sold, which effects are allowed to be sold in most of the countries in the world – the swastika used by the Nazis have for centuries also been used by in Africa and Asia.[71] Why shall American Yahoo! Inc. and its CEO be punished for acting as an intermediary about something Frenchmen could just as well have seen via satellite TV, which latter until now has not been punished by countries where it for example is prohibited and banned to show movies containing pornographic scenes. In such incidents is it the TV-canal itself that has decides the broadcasted content, contrary to Yahoo. The international society had until now not allowed

[70] See further this book Chapter 7.

[71] The Swastika has Greek and Celtic roots. It has also been used in Buddhism and Jainism. For example it is the Buddhist flag in Korea. It has also been used at Sri Lanka as symbol for Red Cross. It is commonly seen in Indian artwork. Only the European Union has urged to ban the swastika because of its Nazi associations with hate and racism.

each country universal jurisdiction over content on satellite TV and thereby not agreed upon allowing the most restricted and limited community to determine the content on satellite canals. Quite the opposite, the international society has referred each country to see to it that only its own citizens has to comply with its legislation, for example by having installed a special filter-chip in their TVs, so they cannot receive prohibited canals.

Transferred to the Internet, the international society ought to prohibit all countries from determine on exterritorial conduct and acts on the Internet (global jurisdiction[72]) and demand that each country – if wanted by this – require only of its own citizen's computers that these are equipped with hardware and/or software, which hinders access to forbidden webpages. This is technically possible as far as the country's citizens does not violate the law and achieves access to the international computer networks by circumventing the by law demanded hardware or software – as it has been the case in China having a national firewall that is anyhow circumvented by the citizen by accessing the Internet (without using the mainland's phone lines and in stead) using mobile phones to satellites.[73]

If the international community chooses to allow universal or global jurisdiction over the Internet, this will imply that for example the Danish nationwide newspaper "Ekstrabladet" must remove its "page 9-girl", which without doubt is regarded as offensive in several countries. Thus, the Danish constitutional liberty of the press will be substantial restricted and in future will have to comply with the country, which has the most stringent and inflexible laws on the press.

The ultimate result would be that what is legal in the brick and mortar world, would most highly likely not be allowed on the public international computer networks (the Internet), which then would be govern by the rule of

[72] See this book Chapter 3 sections 3.3.1. and 3.3.4.

[73] As of November 2005, every fifth Chinese had a mobile phone, in total 383 millions, pursuant to the Chinese Ministry of Information Industry, INQ7 Interactive, Inc, November 23, 2005, <http://news.inq7.net/infotech/index.php?index=1&story_id=57498> (visited March 2006). By the end of 2005 China had 111 million Net users, see survey released by the China Internet Network Information Center <http://www4.cnnic.net.cn/en/index/> (visited January 2006).

the State in the world that has the most limiting law in the world. This would undoubtedly imply nearly the death of the Internet as an (international) information-media. And anyhow, this does not mean that the same persons, which is offended or upset by something in Cyberspace and therefore wants it forbidden, will avoid seeing or experiencing the same during a visit in a foreign country.

As for the *S.S. Lotus* case[74] should be remarked, that this case today would have had another result, because the U.N. treaty on the High Sea states, that the flag state has exclusive jurisdiction on the High Sea over ships that sail under its flag.[75] It might be an idea to regard the Internet as an "internationals sea-area" and copy the rules on jurisdiction from before mentioned treaty on the High Sea.

6.9. Final Remarks

The Yahoo case has far-reaching effect and for the sake of the Internet as a public international media, which is appraised by "we, the representatives of the peoples of the world, assembled" at the U.N. world summit on the information society,[76] one could only had hoped that the American Yahoo appeal court would have decided to deal with the subject matter, and that the court then would have based its decision on public international law and the Internet's international technicality.[77]

If the U.S. appeal court had decided to affirm the decision from the lower court, then the dilemma could have ended up before the International Court of Justice, which seems to have been a reasonable - or maybe necessary - step, as Nations in the world probably will not stop their present habit of dealing with exterritorial Cyberspace issues before the ICJ (hopefully) has stated that such states violate public international law (confer the U.N. Decla-

[74] *S.S. Lotus* (France v. Turkey), 1927 P.C.I.J (Ser. A) No. 10. Also at <www.geocities.com/hssph/Lotus.doc>.

[75] Article 92 (1) of the United Nations Convention on the Law of the Sea of 10 December 1982, U.N. Doc. A/CONF.62/122.

[76] WSIS Declaration of Principles of 12 December 2003, WSIS-03/Geneva/Doc/4-E and Tunis Commitment of 18 November 2005, WSIS-05/TUNIS/DOC/7 –E.

[77] See page 510-518 in SPANG-HANSSEN *supra* note 9.

ration on free speech).

As for the criminal case in France, here public international law has been violated and the international technical aspects of the Internet unfortunately did not seem to have influenced the French courts as it should have. However, as the defendant have been relieved of all charges, thus, that part of the international dilemma must be regarded as moot.

As for public international computer networks it is evidently and clear that the courts for a long period – if not eternally because of the fact that the computer technology changes every half year – will have fundamental and basic problems with securing that the court's decision is not exterritorial and build on the right fully technical assumption and preconditions. A example of the later is an American case that has been nearly in "regular service between" a Circuit Court and the U.S. Supreme Court, as none of the courts until now (four times)[78] has wanted to hold that there exists sufficient safe, valid and durable software, which would allow commercial publishers and editors on the Internet to comply with a U.S. statute, wherefore the statute should not be declared unconstitutional, because it was impossible to obey. The courts has acknowledged that it so far has been impossible to produce filters that can sort pictures or text hidden in picture-files respectively to weed out Mein Kampf but allow Anna Franks diary on the Nazi-period in Germany.

[78] At the latest "returned" by the Supreme Court June 29 2004 as *Ashcroft v. American Civil Liberties Union*, 124 S.Ct. 2783. Previous decisions mentioned page 173-181 in SPANG-HANSSEN *supra* note 9.

CHAPTER 7

CyberCrime Convention Article 22 on Jurisdiction & Public International Law

By Henrik Spang-Hanssen[1]

The Cybercrime Convention of 23 November 2001[2] has in article 22 provisions on jurisdiction. This chapter will discuss the content of article 22 on basis of public international law and previous international instruments dealing with international crimes. It should be noted that the text on the convention in overall has not been formulated by an international committee[3] but by the Council of Europe, wherefore European points of view has had the overall influence on the formulation of the convention.[4] Furthermore, should be

[1] I'll to thank Professor Jiri Toman, Institute of International and Comparative Law, School of Law for comments to this chapter.

[2] By some called the "Budapest Convention ", ETS no. 185 of 23 November 2003 (into force 1. July 2004), at <http://conventions.coe.int/treaty/en/treaties/html/185.htm> [hereinafter Cybercrime Convention]. Chart of signatures and ratifications, Council of Europe at <http://conventions.coe.int/Treaty/Commun/ Cherche-Sig.asp?NT=185&CM=11&DF=22/08/2005&CL=ENG> (visited 22 August 2005).

[3] Stanford University made in 2000 *A Proposal for an International Convention on Cyber Crime and Terrorism* (Draft by George D. Wilson, Abraham D. Sofaer and Gregory D. Grove, Center for International Security and Cooperation (CISAC), Hoover Institution) <http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf> (visited May 2006) [hereinafter STANFORD-PROPOSAL] . Reprinted in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 58 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5). Also available from <http://www.hoover.org/publications/books/cybercrime.html> (visited May 2006) [hereinafter SOFAER].

[4] See the preamble to the Cybercrime Convention *supra* note 2.

noted that the Council of Europe to a very large extent consists of the Council of the European Union.[5]

7.1. To what extent can a State Claim Jurisdiction over Cybercrimes under public international law?

7.1.1. What is a Cybercrime?

At first one has to ask what should establish a "Cybercrime"?[6] Immediately comes to mind that one has to consider the following issues related to computers: Identity theft and invasion of privacy,[7] Internet fraud,[8] ATM fraud, wire fraud, file sharing and piracy, counterfeiting and forgery, child pornography,[9] hacking, computer viruses, denial of service attacks, spam,[10] sabo-

[5] For the record, some other Nations were invited to participate in the drafting.

[6] See also IP Security Attacks in chapter 2 secrtion 2.6.1 and Adv. Rohas Nagpal, *Tools and techniques of cybercrime*, Asian School of Cyber Laws at <www.asianlaws.org/cyberlaw/library/cc/cc_tt.htm>. A COMPUTER CRIME SURVEY of 2005 from FBI can be found at <www.fib.gov/publications.ccs2005.pdf> (visited January 2006).

[7] Spyware impairs "users' control over material changes that affect their user experience, privacy or system security; use of their system resources, including what programs are installed on their computers; or collection, use and distribution of their personal or otherwise sensitive information," the Anti-Spyware Coalition <www.antispywarecoalition.org>, Ryan Singel, *Giving New Meaning to 'Spyware'*, WIRED NEWS 12 July 2005 at <http://www.wired.com/news/privacy/0,1848,68167,00.html>. A guidance on Internet Security at <www.steptoe.com/publications/365b.pdf> (visited May 2006).

[8] A FBI survey shows the biggest frauds are: auction-fraud (62.7 %) and Non-deliverey (15.7 %) and Credit/debit Card (6.8 %), IC3 2005 INTERNET CRIME REPORT, Internet Crime Complaint Center p. 7 <www.ic3.gov> or <www.fbi.gov/publications/ccs2005.pdf> (visited May 2006).

[9] Child pornography is only a crime in a small number of countries. A global legislative overview can be found in CHILD PORNOGRAPHY: MODEL LEGISLATION & GLOBAL REVIEW 7-27 (International Centre for Missing & Exploited Children 2006) at <http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf>.

tage, phishing,[11] pharming,[12] keylogging[13] and zombie[14] computers.

[10] In the last quarter of 2005, 46.8 % of all spam came from the U.S. and China (nearly equally), <www.sophos.com/pressoffice/news/articles/2006/01/dirtdozjan05.html> (visited February 2006).

[11] Phishing is a form of criminal activity using social engineering techniques characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is typically done using email or an instant message, for example disguised as an official email from a (fictional) bank, which attempts to trick the bank's members into giving away their account information by "confirming" it at the phisher's linked website. However, Phishing might be passé as Keylogging has come up.

[12] Pharming is the exploitation of a vulnerability in DNS server (machines responsible for resolving internet names into their real addresses) software that allows a cracker to acquire the domain name for a site, and to redirect, for instance, that website's traffic to another web site. If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN number or account number. However, this is only possible is the original site is not SSL protected, or when the user is ignoring warnings about invalid server certificates. SSL (Secure Sockets Layer and its successor Transport Layer Security (TLS)) is a cryptographic protocol, which provides secure communications on the Internet, see RFC 2246 and RFC 4346.

[13] Keylogging or Keystroke logging - a diagnostic used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems. Such systems are also highly useful for law enforcement and espionage - for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. However, keyloggers are widely available on the Internet and can be used by anyone for hacker purposes. It is possible to install a keystroke logger without getting caught and downloading data that has been logged without being traced. There is no easy way to prevent keylogging. The best strategy is to use the common sense and a combination of several methods, including observing the programs which are installed, being aware of devices connected to USB ports, and enabling firewalls.

[14] A computer attached to the Internet that by a security cracker has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks. The hacker sends commands to the zombie through an open port. Compared to programs such as viruses or worms that can eradicate or steal information, zombies are relatively benign as they only temporarily cripple a targeted Web site by on command sending an enormous amount of packets of useless information to the targeted Web

There is no doubt that virus spread in a computer network is not wanted by anyone, but this does not necessary make it a crime, as it can also be a weapon in wars of the future[15] ("Information Warfare weapon", IW).[16]

Many military officers and at least one President's Directive[17] acknowledge that future wars will not be won with use of conventional weapons or

site in order to clog the site's routers and keep legitimate users from gaining access to the site, but they do not compromise the site's data. Between 50% and 80% of all spam worldwide is now sent by zombie computers, whereby spammers avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth. For taking control of 400,000 Internet-connected computers and renting access to them to spammers and fellow hackers a *21-year-old hacker sentenced to nearly 5 years in prison*, SILICONVALLEY.COM 9 may 2006 at <www.siliconvalley.com/mid/siliconvalley/news/editorial/14537874.htm> (visited May 2006).

[15] On Information Warfare, see HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION chapter 14 (DJØF Publishing, Copenhagen 2004 – 87-547-0890-1 – US Congress Library 2004441311) [hereinafter SPANG-HANSSEN].

[16] A question is whether Article 2(4) of the U.N. Charter prohibiting use of force also embraces electronic computer attacks. If not, the States have a loophole for circumventing the article and use (modern) force. See also, Christopher C. Joyner and Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 Eur.J.Int'l.L 825 (2001), Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 New York Journal of International Law and Polities 57 (2001), Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Columbia Journal of Transnational Law 885 (1999), Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 Harvard International Law Journal 272 (1996).

[17] In July 2002 George W. Bush as the first U.S. president signed a National Security Presidential Directive (NSPD 16) ordering a national-level guidance for determining when and how the United States would launch Cyber-attacks against enemy computer networks by penetrating and disrupting foreign computer systems with a the strategic doctrine similar to that has guided the use of nuclear weapons since World War-II, that is, the principles of proportionality and discrimination – thus sending a computer virus through the Internet to destroy an enemy network would be ruled out as too blunt a weapon <http://www.fas.org/irp/offdocs/nspd> (visited May 2005). See also SPANG-HANSSEN *supra* note 15, at 114-15.

bombs, but by the country that has the best computer experts.[18] Thus, military in different nations are employing people[19] to attack other countries' computer networks so other countries main computers can be infiltrated or network destroyed or made useless by DoS[20] or Ping of Death.[21]

Hacking[22] can be regarded as a crime, as a military weapon or as a mean for supporting human rights. For the latter should be mentioned, that at the latest many people have realized that a most important weapon in the struggle

[18] War crime is a crime (as genocide or maltreatment of prisoners) committed during or in connection with war, Merriam-Webster OnLine at <http://www.m-w.com/dictionary/warcrime>. See *also* definition in article 8 of the Rome Statute of the International Criminal Court of 17 July 1998 (Into force on 1 July 2002), 2187 U.N.T.S. 3 (English text with corrections 1998-2002 at 90), also at <http://www.un.org/law/icc> or <http://www.icc-cpi.int>. As of May 2006 139 signatories and 100 parties, at <http://untreaty.un.org/ENGLISH/bible/englishinternetbible/partI/chapterXVIII/treaty11.asp> [hereinafter ICC-Statute].

[19] North Korea has 600 computer hackers to launch cyberattacks and surveillance equal to the U.S. CIA, *N. Korean Military Hackers Conduct War in Cyberspace*, CHOSUN May 27, 2004 at <http://english.chosun.com/w21data/html/news/200405/200405270038.html>, *N. Korea's Hackers Rival CIA, Expert Warns*, CHOSUN June 2, 2005 at <http://english.chosun.com/w21data/html/news/200506/200506020014.html> and Soo-jeong Lee, *North Korea has 600 computer hackers, South Korea claims*, SECURITYFOCUS October 5, 2004 at <www.secutiyfocus.com/news/9649> (all visited June 2005).

[20] See Appendix N, Definitions & abbreviations in SPANG-HANSSEN *supra* note 15.

[21] One scholar has even suggested that a state can enforce its decisions and sanctions by hacker tools like viruses and worms against "offenders" in foreign States, Joel Reidenberg, *Technology and Internet Jurisdiction*, 153 U.Pa.L.R. 1951, 1963 (June 2005). However, this suggestion goes far beyond what is legal under public international law, *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) of June 27, 1986, 1986 I.C.J. 14.

[22] Hacking: To alter a computer program or to gain access to a computer file or network illegally or without authorization done by a "cracker"; or to legally solve problems with a computer or programs by an expert <http://www.thefreedictionary.com/hacking+around>, <http://www.m-w.com/dictionary/hacker>, <http://www.m-w.com/dictionary/cracker>, <http://www.webopedia.com/TERM/H/hacker.html> and <www.asianlaws.org/cyberlaw/library/cc/hacking.htm>..

for human rights is computer code. Thus, "hacktivism" has turned up in shape of elite computer experts – the "original" hackers, not crackers[23] - who have set their sights on ways to help human-rights causes and are trying to give activists electronic ways to circumvent government surveillance and information management.[24] Such humanitarian help can probably not qualify being a crime – at least there is a lack of the necessary criminal intent.

Finally, as for on-line content should be pointed out, that what in one country might be illegal, can be totally legal in another.

From the perspective of the author as previously working as a district attorney it is of course preferable for the police and prosecution to have jurisdiction over any crime pursuant to ones own laws. However, aspects such as privacy should limit to what extent a country can claim jurisdiction for acts done legally abroad. Additional, due process under public international law requires that a cybernaut can predict in which jurisdiction he can be sued. In this respect should also be remembered, that many cybercrimes are done by minors[25] that have no expectation of criminal procedure in foreign counties

[23] "Cracker": A person who illegally gains access to and sometimes tampers with information in a computer system. See also SPANG-HANSSEN *supra* note 15, at 112 footnote 303. ScatterChat is a Hacktivist weapon designed to allow non-technical human rights activists and political dissidents to communicate securely and anonymously while operating in hostile territory. It is also useful in corporate settings, or in other situations where privacy is desired, see American Electronic Frontier Foundation (EFF) on Tor (an anonymous Internet communication system) at <http://tor.eff.org> and <http://www.scatterchat.com>.

[24] SPANG-HANSSEN *supra* note 15, at 102.

[25] For example in February 2006, 9 out of 55 arrested were minors. They had used keylogging programs for recording unwitting Brazilians keystrokes whenever these visited their banks online. The programs sent the stolen users names and passwords back to members of the gang, which stole about $4.7 million from 200 different accounts, Tom Zeller, *Cyberthieves Silently Copy Your Passwords as You Type*, THE NEW YORK TIMES 27 February 2006 at <http://www.nytimes.com/2006/02/27/technology/27hack.html> (visited May 2006). In March 2006 a 14 year old boy found a javascript vulnerability in Google's gmail, which information he posted on a webblog – and thus to the whole world - rather than informing Google about the security breach, see <http://ph3rny.blogspot.com/2006/03/vulnerability-in-gmail.html> and <http://isc.sans.og/diary.php?storyid=1161> (visited 3 March 2006).

and often are underage with respect to criminal statutes. Finally, it is questionable whether a foreign country should have criminal jurisdiction over an alien, which of human-rights causes circumvents the foreign government's surveillance and information management as long as he does not enter that foreign country and the acts were legal in the country where the act was done. This would be against the U.N. Declaration on Human Rights.

As for copyright and circumventing the zoning feature in DVD-hardware, it can be questioned whether this should be illegal in all countries, as the Hollywood DVD-Zones after the extension of the E.U. in May 2004 does not correspond to the European Single Marked, since the three Baltic countries is in another DVD-zone than the rest of the E.U. member states. Thus, E.U.-consumers have to carefully check whether the DVD they buy, can be played on the DVD-player they own. This situation is contrary to the Single Market and it can be questioned whether consumers are allowed to circumvent the DVD feature so they can use any DVD they can buy in the E.U. Single Market. Thus, the extension of new members of the E.U. has made present DVD-copyright protection-statutes contrary to principal and essential articles in the main E.U. treaties.[26]

Spam[27] and cookies[28] can be very annoying, but it is questionable whether

[26] Henrik Spang-Hanssen, *Hollywood puts 3 Baltic countries into a Second Class of E.U. or Hollywood does not recognize E.U.'s single market from May First 2004* at <www.geocities.com/hssph/articles>. France has in June 2006 changed its copyright law that might force Apple Computer to make songs purchased from its market-leading iTunes Music Store compatible with music players of it rivals, Thojmas Crampton, *Paris Approves Law Aimed at Making iTunes Compatible With Rival Devices*, THE NEW YORK TIMES, 1 July 2006, at <www.nytimes.com/2006/07/01/business/worldbusiness>.

[27] See definition above chapter 3, footnote 221. Spam will probably continue to be a large phenomen in Cyberspace, see SECURITY THREAT MANAGEMENT REPORT 2005 p. 9, Sophus at <www.securitymanagement.com/library/trojans_sophos0206.pdf> (visited May 2006).

[28] See SPANG-HANSSEN *supra* note 15, at 524 footnote 1850 and at Appendix N, Definitions & Abbreviations. A company has developed a product (Persistent Identification Element – PIE) to restore the cookies set by web sites, ad networks and advertisers when users try to delete them, *Tool can resurrect deleted cookies*, Out-Law 5 April 2005 at <http://www.out-law.com/page-5502> (visited May 2006). In January 2006 a newspaper in the U.S. found out that many official websites used Web bugs or cookies

they always imply a crime. Spam from one person target against a certain individual or company can be a crime.[29] On the other hand, spam can be regarded as electronic unsolicited advertising and thus an online business

to track web visitors, Declan McCulagh, *Government Web sites are keeping an eye on you*, CNET NEWS.COM 5 January 2006 <http://news.com.com/2100-1028_3-6018702.html> (visited January 2006).

[29] *Rigsadvokaten* (US: Attorney General) *v. Teleselskabet* [tele-company] *Debitel*, UfR 2005.3446 H (Danish Supreme Court, 22 September 2005) (T send 12,000 SMS-messages and 36,000 e-mails to certain receivers with purpose of selling services. Penalty of 2 million DKK (~ $308,000) for causing the recievers a nuisance, the improper formulation in the e-mails, and the gained profit. SMS-messages not regarded as "electronic mail"). *Ferguson v. Friendfinders, Inc*., 94 Cal.App.4th 1255 (California Court of Appeal, 1st Dist, Jan 2002)(Statute valid as did not discriminate against or directly regulate or control interstate commerce. The state had a substantial legitimate interest in protecting its citizens from the harmful effects of deceptive unsolicited commercial e-mail) and *MaryCLE v. First Choice Internet, Inc*., 166 Md.App. 481, 890 A.2d 818 (Court of Special Appeals of Maryland, Jan. 26, 2006)(E-mail recipient and Internet service provider brought action against out-of-state internet marketing company alleging violations of the Maryland Commercial Electronic Mail Act. Held that exercise of jurisdiction over out-of-state company did not violate due process and that statute did not violate Dormant Commerce Clause as applied to marketing company), but *declined to follow* by *Dring v. Sullivan*, 423 F.Supp.2d 540 (D. Md., Mar 30, 2006). *Commonwealth of Virginia v. Jeremy Jaynes* (Circuit Court of Virginia, Loudoun County - Judge Thomas D. Horne, November 2004 - Criminal Nos 15885, 15886, 16121) (9 years for illegal spamming. Jaynes, who was considered among the top 10 spammers in the world at the time of his arrest, used the Internet to peddle pornography and sham products and services such as a ""FedEx refund processor," prosecutors said. Thousands of people fell for his e-mails, and prosecutors said Jaynes' operation grossed up to $750,000 per month. He was convicted for using false Internet addresses and aliases to send mass e-mail ads through an AOL server in Loudoun County, where America Online is based. Under Virginia law, sending unsolicited bulk e-mail itself is not a crime unless the sender masks his identity. While prosecutors presented evidence of just 53,000 illegal e-mails, authorities believe Jaynes was responsible for spewing out 10 million e-mails a day) Matthew Barakat, *Judge Sentences Spammer to Nine Years*, AP 2 April 2005 at <http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/04/08/financial/f100816D42.DTL>, *confer* 64 Va. Cir. 443, 2004 WL 1166933 (Va. Cir. Ct. May 25, 2004) and 65 Va. Cir. 355, 2004 WL 2085359 (Va. Cir. Ct. Aug 11, 2004).

method and thus not a crime.[30] So far many court decisions have relied on the fact that the cybernaut knew that a certain network or notes would have great difficulties with handling the amount of unsolicited advertising. But is it a crime that a delivering system is "overwhelmed" with unsolicited advertising? Furthermore, in some countries certain kinds of spam and cookies (the U.S.) are allowed, whereas it is illegal in other countries without previous given permission by the receiver (the E.U.).[31] For spam and cookies, which is usually generated by computers and thus without human interference, it is questionable whether there can be proven the necessary criminal intent by a person as for the country that want to claim jurisdiction.

As for acts done "purely online"[32] on international computer networks - where anything first uploaded can be accessed be anyone connected to the Internet - it should be considered whether the requirement of a close connection and reasonableness in public international law on jurisdiction is fulfilled. In relation to acts done on international computer networks there should be made restricted interpretation of statutes so it is required, that the act behind the violation has been aimed at the country claiming jurisdiction and that it is

[30] *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 71 P.3d 296, 1 Cal.Rptr.3d 32 (Supreme Court of California, Jun 30, 2003)(Employer filed action against former employee who flooded employer's e-mail system. Held that: (1) tort of trespass to chattels did not encompass electronic communications that neither damaged the recipient computer system nor impaired its functioning; (2) temporary use of some portion of employer's computer processors or storage by former employee's e-mail messages was not an injury to employer's interest in its computers, as was required to support claim for trespass to chattels; (3) consequential economic damage employer claimed to have suffered was not an injury to employer's interest in its computers; (4) common law would not be extended to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents were objectionable; and (5) even assuming corporate employer could under some circumstances have claimed a personal constitutional "right not to listen," former employee did not violate right), *distinguished* by *School of Visual Arts v. Kuprewicz*, 3 Misc.3d 278, 771 N.Y.S.2d 804 (N.Y.Sup. Dec 22, 2003) and *Sotelo v. DirectRevenue*, LLC, 384 F.Supp.2d 1219 (N.D.Ill. Aug 29, 2005).

[31] Laws that may appear to be similar or identical may be enforced differently, Tonya L. Putham & David D. Elliott, *International Responses to Cyber Crime in* SOFAER *supra* note 3, at 58. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/35.pdf >.

[32] Above page 1 and SPANG-HANSSEN *supra* note 15, at 298.

reasonable pursuant to basic international law on jurisdiction that for example a Danish court deal with the case.[33] Maybe there should also be made a distinction between incidents where the injury is related to a natural person and incidents concerning a business.

> *Viasat A/S and Canal Digital Danmark A/S v. A* (Danish citizen with residence in Columbia), UfR 2002.405 H (Supreme Court of Denmark, 27 November 2002) - A Dane living aboard and without any location in Denmark edited the website <www.piratdk.com> placed on a server outside Denmark. From the website could be downloaded material that was illegal in Denmark. The website was Danish languaged and concerned Danish encryption keys. Held, Rpl. §243 cannot be used in cases where the claim is an injunction.
>
> Similar case in *Canal Digital Danmark A/S v. Hans Magnus Carlsson*, UfR 2001.2186 Ø (Easter Appeal Court 26 June 2001).

7.1.2. When does a State has jurisdiction over a cybercrime under public international law?

Public international law does not allow exercise of so-called "Global Jurisdiction".[34] It would bring chaos on international computer network, if every State could legislate about content on foreign websites and through its courts make judgments against aliens whom were held to have made a violation of that State's law. For example as for the Danes, it would imply that the content of Danish websites, which were in accordance with Danish law after the liberalization of prohibition of some pornography provisions, but which sites constituted a violation in foreign countries, could be punished there.[35] If so, Danes could be arrested at (catholic) southern European holiday-destinations or in the U.S. on basis of their websites' content, which foreigners cannot be

[33] SPANG-HANSSEN *supra* note 15, section 32.1.1.1., 32.2., and Chapter 34.

[34] See above chapter 3 section 3.1.1, IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 299-305 (6th Edition, Clarendon Press, Oxford – ISBN 0199260710) [hereinafter BROWNLIE], ANTONIO CASSESE, INTERNATIONAL CRIMINAL LAW 277-300 (Oxford University Press – ISBN 0-19-925911-9)[hereinafter ANTONIO CASSESE].

[35] Another example is the French-US Yahoo case, which is thoroughly reported in SPANG-HANSSEN *supra* note 15, 184-189, 463-466 and 483-517. See also chapter 6.

prohibited to see (unless access is prohibited at large costs if at-all possible). In this context it is troubling that the U.S. claim that it has personal jurisdiction for circa 70 percent of what happens on the international computer networks, because circa 70 percent of the networks serves are placed in the U.S.[36] Furthermore, does this allow the U.S. to make surveillance of e-mail correspondence or allow U.S. to claim jurisdiction? It is doubtful whether a cybernaut has had any thought about the U.S. placed servers and thus has had the necessary criminal intent related to the U.S. A citizen in the E.U. might very possible rather have in mind article 25(1) of the E.U. Data Protection Directive,[37] which provides that computerized data may be transferred to a third party country only if that country ensures an adequate level of protection for personal data.

It should be pointed out that law-scholars/politicians have not been able to make a solution on jurisdiction and enforcement.[38] A workable solution related to Cyberspace can only be achieved if technical network aspects are taking into account, thus requiring participation of computer technicians in drafting jurisdictional rules related to Cyberspace[39] - no government has ever legislated on cars without thoroughly consulting car-technicians, but as to Cyberspace-legislation technicians have so far not been invited. It is characteristic for conferences dealing with the international public networks that they lack the participation of both computer technicians and international public law scholars. For example, the attempt to make a convention on Jurisdiction and Enforcement was only participated by national public servants or private international law scholars.[40] Before computer technicians and international public law scholars are invited to the same table, it is unrealistic to presume that fair cross-border rules accepted by the international society will

[36] Compare the legislation related to the USA Patriot Act of 2001 ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of October 26th 2001), 2001 PL 107-56 (HR 3162), 18 U.S.C. § 2510 – 2511.

[37] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23/11/1995 p. 0031 – 0050.

[38] See SPANG-HANSSEN *supra* note 15, section 33.6.

[39] See SPANG-HANSSEN *supra* note 15, Chapter 35.

[40] See SPANG-HANSSEN *supra* note 15, section 33.5.

be accepted.

A state has only jurisdiction over aliens on basis of either the subjective territoriality principle or the active personality principle, and to a limited degree the objective territoriality principle. In very special instances can the state act on behalf of the whole world and thus be allowed to use the universal jurisdiction principle. I all cases exercise of jurisdiction has to be reasonable.[41]

Under customary public international law an individual may be considered criminally responsible only for conduct which was unambiguously criminal at the time of its commission and must be sentenced in accordance with law.[42] It has four essential attributes:[43]

- the concept of a written law,
- the value of legal certainty,
- the prohibition on analogy, and
- non-retroactivity.

There exists no rule under customary public international law requiring a state to surrender a person within its boundaries to a prosecuting state – not even if it does not punish the individual. On the contrary, states have always upheld their rights to grant asylum to foreign individuals as an inference from their territorial authority, except where the requested state is a party to a treaty with the requesting state.[44]

[41] See SPANG-HANSSEN *supra* note 15, at 244-257, BROWNLIE, *supra* note 34, at 299-305.

[42] "The principle of legality" consisting of *Nullum crimen sine lege* and *Nulla poena sine lege*.

[43] THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY 733-66 (Ed. Antonio Cassese, Oxford University Press 2002 – ISBN 0-19-829862-5) [hereinafter CASSESE].

[44] OPPENHEIM'S INTERNATIONAL LAW 950 (London and New York: Longman 9th Ed., paperback edition 1996 – ISBN 0582302455) [hereinafter OPPENHEIM], and BROWNLIE, *supra* note 34, at 313-14. Otherwise JORDAN J. PAUST, INTERNATIONAL LAW AS LAW OF THE UNITED STATES 405 (Carolina Academic Press 1996 – ISBN 0890898626) [hereinafter PAUST]

7.2. Universal Jurisdiction

Universal Jurisdiction as mentioned above in chapter 3 section 3.3.2 can only be used by a State or its courts if the international society has allowed its use and if so only for the very small number of specific serious offences[45] that the international society has allocated to universal jurisdiction. That is, there exist serious offences that the international society has not allowed universal jurisdiction for.

This kind of jurisdiction can by used by a State's court even if the State of the court has no legislation for its use,[46] because the court acts on behalf of the whole world.[47] It should not be used for political purposes, but only where there is a fundamental interest of the international community as a whole. Thus, the jurisdiction is bases solely on the nature of the crime, not in the interest of the single victim or single group of States.

Furthermore, the use of universal jurisdiction requires observance of international – not national – due process norms, including rights of the accused and victims, the fairness of the proceedings, and the independence and impartiality of the judiciary.[48]

The universal jurisdiction forbids multiple prosecutions or punishment for the same conduct and that States shall recognize the validity of a proper exercise of universal jurisdiction by another State and shall recognize the final judgment.[49]

[45] THE PRINCETON PRINCIPLES only lists seven, see principle 2.1 (confer principle 2.2), at <www.princeton.edu/~lapa/unive_jur.pdf> (visited November 2005) [hereinafter THE PRINCETON PRINCIPLES]. See also Amnesty International, UNIVERSAL JURISDICTION (2001)(AI Index: IOR 53/002/2001) at <www.amnesty.org> or <www.iccnow.org>. BROWNLIE, *supra* note 34, at 303-305

[46] *Id.* principle 3.

[47] SPANG-HANSSEN *supra* note 15, at 252-54, OPPENHEIM *supra* note 44, at 469-70 and PAUST *supra* note 44, at 392-93.

[48] THE PRINCETON PRINCIPLES *supra* note 45, principle 1.4.

[49] *Id*. principles 9.1 og 9.2 (the principle of "Non Bis In Idem"). This principle is also formulated in article 20 of the ICC Statute *supra* note 7. See also OPPENHEIM *supra* note 44, at 469-70 and BROWNLIE *supra* note 34, at 303 and Restatement (Third) of Foreign Relation Law § 404 on Universal Jurisdiction and § 423.

7.3. U.N. Convention Against Transnational Organized Crime

The "Palermo Treaty"[50] cannot be regarded as a codification of customary international law and therefore "universal jurisdiction" cannot be used in relation to - at least - several of the crimes that the convention deals with. It should be pointed out, that the convention itself does neither use the term "universal jurisdiction". Furthermore, even though the convention uses the term "serious crimes", this does not allow exercise of universal jurisdiction as it is for, and only for, the international society as a whole to decide which specific "serious crimes" allow use of universal jurisdiction.

Thus, the convention's rules, and especially the jurisdiction rules, are only valid under public international law between the State parties. Furthermore, pursuant to the convention's text does it only apply to the prevention, investigation and prosecution of:[51]

A. Offences specified in articles 5 (conspiracy,[52] participation in an organized criminal group), 6 (conversion or transfer of property for the purpose concealing or discussing the illegal origin of the property, e.g. money laundering), 8 (corruption of public official(s)) and 23 (obstruction of justice (induce false testimony, produce false evidence, intimidate or threat judges or law enforcement officers); or

[50] The "Palermo Treaty" or United Nations Convention Against Transnational Organized Crime" of 2000 (CTOC) (into force on 29 September 2003), A/RES/55/25 at <http://www.unodc.org/unodc/en/crime_cicp_resolutions.html>. As of 23 November 2005: 147 signatories and 119 parties: at <http://www.unodc.org/unodc/en/crime_cicp_signatures_convention.html> (visited May 2006) [hereinafter PALERMO TREATY]. The U.S. became a party on December 3, 2005. The CTOC and its protocols (COP) are supported by the U.N. Commission on Crime Prevention and Criminal Justice <www.unodc.org/unodc/en/crime_cicp_commission.html>. See also U.N. Crime and Justice at <www.uncjin.org> and Vienna Declaration on Crime and Justice of 17 January 2001, U.N. Doc. A/RES/55/59 at <http://www.unodc.org/pdf/crime/a_res_55/res5559e.pdf>.

[51] PALERMO TREATY *supra* note 50, article 3.

[52] The Danish Civil Penal Code does not know of the terms "Conspiracy" or "Participation in a criminal organization", but such acts might be penalized as accessory to a crime pursuant to §23 of that Code, Remark to § 5 of the bill no. 5 of 23 October 2004, enacted as §5 in law no. 1434 of 22 December 2004.

B. "Serious crimes" defined in article 2, that is, conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.[53]

The convention defines an offence as "transnational" if:[54]

- The offence is committed in more than one State
- It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in an-other State
- It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
- It is committed in one State but has substantial effects in another State.

Each party to the Convention shall establish jurisdiction over offences pursuant to article 5, 6, 8 and 23 when:[55]

(a) The offence is committed in the territory of that State Party; or

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.

Subject to article 4 (protection of sovereignty)[56] of the Convention, a State Party may also establish its jurisdiction over any such offence when:[57]

(a) The offence is committed against a national of that State Party;

(b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory; or

(c) The offence is:

[53] This can easy be achieved in an American court where each offence is separately decided and simply added (e.g. 4 life time sentences); whereas other Nations decide the sentence as a lump or have statutes maximize a life time sentence (e.g. Denmark with a maximum of 16 years imprisonment (life in very extreme cases)).

[54] PALERMO TREATY s*upra* note 50, article 3(2).

[55] *Id.* article 15(1).

[56] *Id.* article 4: (1) States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States; (2) Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

[57] *Id.* article 15(2).

(i) One of those established in accordance with article 5, paragraph 1, of this Convention and is committed outside its territory with a view to the commission of a serious crime within its territory;

(ii) One of those established in accordance with article 6, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 6, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory.

If an offence pursuant to the convention is punishable under the domestic law of both the requesting State party and the requested State party, and the person who is subject of the request for extradition is located in the territory of the requested State party, shall – if the conditions provided for by its domestic law including treaty is fulfilled - either bring the offender before its own courts[58] or extradite the person.[59] However, the requested party can reject to extradite if it has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, religion, nationality, ethnic origin or political opinions or that compliance with the request would cause prejudice to that person's position for any one of these reasons.[60]

The convention does not have any provisions on concurrent jurisdiction or

[58] *Id.* article 15(3) and (4). Each State party shall adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals; and it may adopt measures when the alleged offender is present in its territory and it does not extradite him or her.

[59] Extradition can imply far more severe sentenced that would be given a violator by the extradition-state itself. For example in some European countries are the maximum penalty prison for life, which is equal to 16 years imprisonment, whereas in the U.S. computer hacker that admitted hacking into systems, but denied causing any damage, can face up to seventy years in jail, *Judge: Extradite 'Super-hacker' to US*, THE SCOTSMAN 11 May 2006 <http://thescotsman.scotsman.com/international.cfm?id=704082006> (visited May 2006).

[60] *Id.* article 16.

rather the principle of "*Non Bis in Idem*."[61] However, when drafting the convention there were between experts expressed concern about subjecting individuals to double jeopardy.[62] It was held, that conflicts of jurisdiction were rather rare and were invariably resolved at the practical level by an eventual determination of which jurisdiction would be ultimately exercised on the basis of the chances for successful prosecution and adjudication of the particular case.[63]

However, concurrent jurisdiction is more than likely to happen when the issue is related to computer network where acts nearly always will cross borders.[64] Therefore the rules in this convention do not seem fit to be used for – or by analogy – to Cyberspace incidents. Furthermore, scholars that belong to the source-category of ICJ article 38(d)65 holds that there in public international law is a requirement against "double criminality" in connection to extradition and furthermore, that extradition is only appropriate for more serious offences.[66]

[61] See OPPENHEIM *supra* note 44, at 463-66, BROWNLIE *supra* note 34, at 309 and SPANG-HANSSEN *supra* note 15, at 256, 351, 353, 365, 383 and 501, F.A. Mann, *The Doctrine of Jurisdiction in International La*w, 111 RECUEIL DES COURS 1, 49 (1964-I) [hereinafter MANN-1].

[62] Interpretative notes for the official records to article 16(12) on extradition points out "the action referred to in paragraph 12 would be taken without prejudice to the principle of double jeopardy (neb is in idem)", REPORT OF THE AD HOC COMMITTEE ON THE ELABORATION OF A CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME ON THE WORK OF ITS FIRST TO ELEVENTH SESSIONS, page 6, U.N. Doc. A/55/383/Add.1 of 3 November 2000 at <www.unodc.org/unodc/en/crime_cicp_convention_dociments.html> file 383a1e.pdf.

[63] REPORT OF THE MEETING OF THE INTER-SESSIONAL OPEN-ENDED INTERGOVERNMENTAL GROUP OF EXPERTS ON THE ELABORATION OF A PRELIMINARY DRAFT OF A POSSIBLE COMPREHENSIVE INTERNATIONAL CONVENTION AGAINST ORGANIZED TRANSNATIONAL CRIME page 9 para 29, U.N. Doc. E/CN.15/1998/5 of 18 February 1998 at <www.uncjin.org/Documents/7comm/5e.pdf> (visited 11 May 2006).

[64] See SPANG-HANSSEN *supra* note 15, at 299-300 tables 17-19, 351-2, 365, 383 and 501.

[65] Whereas article 21 of the ICC-Statute *supra* note 18 omits academic writings as a "subsidiary means for the determination of rules of law" and differs further from the ICJ Statute by defining in a relatively precise manner the hierarchy between the different sources it sets out, CASSESE *supra* note 43, at 1076.

[66] OPPENHEIM *supra* note 44, at 957-58 and BROWNLIE *supra* note 34, at 313-318.

7.4. ICC Statute's Jurisdictional Rules

The Statute for the International Criminal Court has not created any entitlements or legal obligations that did not already existed under public international law[67] wherefore it does not violate any principle of the Law of Treaties.[68] The provision in part 3 of the ICC Statute enumerates general principles of criminal law recognized by most national legal systems around the world.[69]

The International Criminal Court does not supersede national jurisdiction, but is rather a complementary that will act when national courts are "unable or unwilling" to perform their tasks.[70] The court – beyond where the U.N. Security Council refers a case – has in principle only jurisdiction where the State of nationality of the accused is a party to the ICC Statute.[71] Furthermore, the court may exercise its jurisdiction over nationals of a non-party State, if the State in whose territory the crime occurred is a Party to the Statute.[72] Thus, the Statute does not allow use of universal jurisdiction – this is partly because some of the crimes in the ICC Statute under public interna-

[67] Roy S. Lee, *Introduction in* THE INTERNATIONAL CRIMINAL COURT: THE MAKING OF THE ROME STATUTE ISSUES, NEGOTIATIONS, RESULTS 29 (Kluwer Law International, 2002 – ISBN 904111212X) [hereinafter LEE], and BROWNLIE *supra* note 34, at 559-575.

[68] Vienna Convention on the Law of Treaties of 23 May 1969, 1155 U.N.T.S. 311(into force 27 January 1980 – As of May 2006: 45 Signatories and 106 Parties) at <http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf> and <http://untreatay/un.org/English/bibl/englishinternetbible/partI/chapterXXIII/treaty1.asp>. There also exists a Vienna Convention on the Law of treaties between States and International Organizations of 21 March 1986, Doc. A-CONF. 129-15 (not yet in force (35 parties needed) – As of May 2006: 38 Signatories and 26 parties) at <http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_2_1986.pdf> and <http://untreaty.un.org/sample/EnglishInternetBible/partI/chapterXXIII/treaty3.asp>.

[69] Herman von Hebel, *Elements of Crimes in* THE INTERNATIONAL CRIMINAL COURT: ELEMENTS OF CRIMES AND RULES OF PROCEDURE AND EVIDENCE 20 (Ed. Roy S. Lee, Transnational Publishers 2001 – ISBN 157105-209-7) [hereinafter VON HEBEL].

[70] Article 17 of the ICC-statute *supra* note 18 carefully define circumstances that govern "inability and unwillingness", LEE *supra* note 67, at 27.

[71] CASSESE *supra* note 43, at 609-610.

[72] Article 12 of the ICC-statute *supra* note 18 and LEE *supra* note 67, at 29 and CASSESE *supra* note 33, at 607-609.

tional law do no qualify for universal jurisdiction.[73]

"A Commentary" holds that there is no reason to believe that the ICC Court could not exercise its jurisdiction if the state of nationality of the alleged perpetrator is not a party to the Statute and one of two states on the territory of which the crime were committed is also not a party to the Statute if just one state is a party.[74] If the State of nationality is not a State party and the State of registration of a vessel or aircraft cannot be identified, then the ICC Court does not have jurisdiction[75] – except if the Security Council refer the case.[76]

However, as for Cyberspace issues the big troublesome question is where the crime occurred. The drafters of the ICC Statute did not take into account that in Cyberspace things can happen everywhere and at the same time. Therefore the wording of article 12(2)(a) of the ICC Statute must be interpretated restricted and curtailed. Thus, the question of "sufficient closeness" and reasonableness under public international law becomes vital for Cyberspace issues, as dealt with in chapter 3 section 3.4. It should be noted that under the ICC Statute the Court does has have jurisdiction for crimes related to non-party States.[77]

[73] CASSESE *supra* note 43, at 535 and 586-607.

[74] CASSESE *supra* note 43, at 567. The argument is reasoned as follows: A crime is committed in whole within the territory when every essential constituent element is consummated within the territory; it is committed in part within the territory when any essential constituent element is consummated there. If it is committed either in whole or in part' within the territory, there is territorial jurisdiction, Harvard Research in International Law, *Draft Convention on Jurisdiction with Respect to Crime*, 29 American Journal of International Law (AJIL) 435, 445 (Supp. 1935).

[75] CASSESE *supra* note 43, at 568.

[76] Article 13(b) of the ICC-statute *supra* note 18.

[77] On May 6, 2002, President Bush formally renounced the U.S.'s obligation as a signatory to the ICC-statute *supra* note 18 to establish an International Criminal Court [hereinafter ICC Court], see U.S. Department of State's ICC-Treaty website at <www.state.gov/t/pm/ris/fs/2002/23426.htm>. "The United States will not recognize the jurisdiction of the International Criminal Court over United States nationals…Any American prosecuted by the International Criminal Court will, under the Rome Statute, be denied procedural protections to which all Americans are entitled under the Bill of Rights to the United States Constitution, such as the right to a trial by jury," 22 U.S.C. 7421 (7) and (11).

The ICC Court only has jurisdiction in cases that involve "the most serious crimes of concern to the international community as a whole"[78] and where the person at the time of the alleged commission of the crime was of the age of 18 or over.[79]

Also should be mentioned that under article 30 of the ICC Statute a person is only criminally responsible or liable for punishment for a crime if the person had "intent", that is (1) the offender meant to engage in the conduct (prohibited act or omission)(actus reus) and (2) the offender meant to cause that consequence or was aware that it would occur in the ordinary course of events (mens rea). Furthermore is required that the crime was committed with knowledge, that is, awareness that a circumstance existed or a consequence would occur in the ordinary course of events.[80]

Under article 25 of the ICC Statute a person is also criminally responsible or liable for punishment if that person for the purpose of facilitation the commission of a crime, aids, aets or otherwise assist in its commission or its attempted commission, including providing the means for its commission. The article does not contain a comprehensive and definite compilation of all requirements essential for individual criminal responsibility.[81] A person is not liable if he completely and voluntary abandoned the criminal purpose before the crime could be executed.[82]

Criminal responsibility is only excluded where there is a mistake of fact if it negates the mental element required by the crime. A mistake of law as to whether a particular type of conduct is a crime within the jurisdiction of the Court is not excluding criminal responsibility.[83] However, a mistake of law may be a ground for excluding criminal responsibility if it negates the mental element required by such a crime, or as provided for in article 33 (about orders given by superior).

[78] Preamble and article 5 of the ICC-statute *supra* note 18.
[79] Articles 26 of the ICC-statute *supra* note 18 and CASSESE *supra* note 43, at 533-35.
[80] VON HEBEL *supra* note 69, at 14-15 and 29, CASSESE *supra* note 43, at 389.
[81] CASSESE *supra* note 43, at 768, 798-801
[82] Article 25 (3)(f) and , CASSESE *supra* note 43, at 807-818.
[83] Articles 32 of the ICC-statute *supra* note 18 and *General Principles of Criminal Law and the Elements of Crimes in* VON HEBEL *supra* note 69, at 36-37 and CASSESE *supra* note 43, at 453-56 and 889-946.

As for crimes under the Statute that could happen in Cyberspace are part of what in article 8 is defined as "war crimes", that would be "Information Warfare", especially paragraph 2(a)(iv) extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly and paragraph 2(b)(xiii) destroying or seizing enemy's property unless such destruction or seizure be imperatively demanded by the necessities of war (e.g. hacker attacks and destruction of central computers regulating traffic).[84]

It should be noted that crimes such as terrorism and drug crimes are not embraced by the Statute. However, Stein Schjølberg has suggested that the International Law Commission should work on a proposal for amendments of the Rome Statute of the International Criminal Court to include cyberterrorism and serious cybercrimes.[85]

7.5. Jurisdiction over Satellites for data transport in Outer Space

Outer Space does not belonging to any state's territory. It can be defined as the lowest limit above the Earth sufficient to permit free orbit of spacecraft without interference from the state below.[86]

The U.N. General Assembly has adopted the view that "international law, including the Charter of the United Nations, applies to outer space and celestial bodies."[87]

[84] VON HEBEL *supra* note 69, at 132 and 170, CASSESE *supra* note 43, at 394, 397-401, 403.

[85] Council of Europe expert on cybercrime & Chief Judge Stein Schjølberg, *Law Comes to Cyberspace*: A presentation at the 11th UN Criminal Congress, 18-25 April 2005, Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime, <http://www.cybercrimelaw.net/documents/UN_Bangkok_05.htm> (visited May 2006). However, the range of this proposal is limited when considering the large extent of computer-use in the U.S. as "no United States Court, and no agency or entity of any State or local government, including any court, may cooperate with the International Criminal Court in response to a request for cooperation submitted by the International Criminal Court pursuant to the Rome Statute." 22 U.S.C. 7423 (b).

[86] The lowest limit would then be 100 miles, BROWNLIE *supra* note 34, at 256.

[87] Resolution 1721 (XVI), adopted 20 December 1961, see also Article 3 of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer

Article 1 of the "Outer Space Treaty" provides that the use of outer space "shall be carried out for the benefit and in the interests of all countries…and shall be a province of all mankind…and shall be free for use by all states without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies." Article 2 provides that outer space "is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or any other means."[88] However, eight equatorial states have claimed that the individual segments of the Clarke Orbit are subject to a regime of national sovereignty, but such claims are difficult to reconcile with article 1 and 2 of the Outer Space Treaty.[89]

The Outer Space Treaty permits the use of communications satellites ("unmanned spacecraft"[90]) for private, that is non-governmental, and even commercial purposes. It is likely that these and some other uses may give rise to a need for regulation, even for some traffic rules, and for dealing with the sort of disputes which must result.[91]

Satellites as part of the communication-chain give special jurisdictional problems and considerations.

Those in the so-called Non-Geostationary Earth Orbit (NGSO) move constantly in relation to the surface of the Earth and their great disadvantage is that they have to be tracked continuously from the ground; whereas satellites

Space, including the Moon and other Celestial Bodies, of 1967, 610 UNTS 205, 18 U.S.T. 2410 (1967)(into force October 10, 1967) [hereinafter Outer Space Treaty].

[88] BROWNLIE *supra* note 34, at 256 and OPPENHEIM *supra* note 44, at 826-845.

[89] The Bogotá Declaration of 3 December 1976 between Brazil, Colombia, Congo, Ecuador, Indonesia, Kenya, Uganda and Zaire (Brazil, Ecuador and Uganda are also parties to the Outer Space Treaty), reprinted at <http://www.jaxa.jp/jda/library/space-law/chapter_2/2-2-1-2_e.html> (visited May 2006), BROWNLIE *supra* note 34, at 259 and OPPENHEIM *supra* note 44, at 841-42.

[90] A spacecraft is designed to leave Earth's atmosphere and operate beyond the surface of the Earth in space. Spacecraft are designed for a variety of missions which may include communications, earth observation, meteorology, navigation, planetary exploration, space tourism and space warfare. The term spacecraft is also used to describe artificial satellites, <http://en.wikipedia.org/wiki/Spacecraft> and <http://en.wikipedia.org/wiki/List_of_spacecraft>.

[91] OPPENHEIM *supra* note 44, at 844.

in the Geostationary (or geosynchronous) Earth Orbit (GSO)[92] will maintain a fixed station over the surface of the Earth.[93] There are over 250 operational geostationary[94] satellites in space, hundreds more are in lower orbits, and that number is increasing.[95] There are uncounted millions of earthstations, ranging from tiny antennas for receiving in mobilphones to 30-m diameter gateway systems. Today, one can buy a GPS receiver to pick up satellite signals for less than $100.[96]

As communications have become automatic and relies less on human intervention, the ability to complete transmissions across borders depends only on achieving compatibility among different kinds of terminal equipment and private and public networks.[97] A report holds that the convergence of mobile communications and the Internet will produce something big, perhaps even the mythical "sum that is bigger than its parts" likely to produce major innovations and thus make the legal jurisdictional issue even more difficult.[98] Furthermore, the emergence of broadband wireless as a platform to provide low-cost high-performance access networks in rural and remote areas[99] will increase the number of end-users – cybernauts - which will be difficult to locate with respect to the jurisdictional issue.

Satellite communication has become an indispensable part of global

[92] Or the "the Clarke Orbit," see footnote 42 above in chapter one section 1.6.

[93] CHARLES H. KENNEDY, AN INTRODUCTION TO INTERNATIONAL TELECOMMUNICATIONS Law 65 (Artech House Inc. 1996 – ISBN 0-890068356) [hereinafter KENNEDY].

[94] See above footnote 92.

[95] MARK R. CHARTRAND, SATELLITE COMMUNICATIONS FOR THE NONSPECIALIST 9 (SPIE PRESS 2004 – ISBN 0-8194-5185-1)[hereinafter CHARTRAND].

[96] CHARTRAND *supra* note 95, at 7.

[97] KENNEDY *supra* note 93, at 37.

[98] Report: ITU and its Activities Related to Internet-Protocol (IP) Networks section 2.8 on Mobile Internet(Version 1.1, International Telecommunication Union, April 2004) at <http://www.itu.int/osg/spu/ip/itu-and-activities-related-to-ip-networks.html> (visited February 2005).

[99] REPORT ON THE DEVELOPMENT OF BROADBAND ACCESS IN RURAL AND REMOTE AREAS OF 10 MAY 2004 - Working Party on Telecommunication and Information Services Policies, (OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, DSTI/ICCP/TISP(2003)7/FINAL) at <www.oecd.org/dataoecd/24/ ??/31718094.pdf> (visited February 2005).

communications.[100] It uses radio waves to carry the information from source to destination and the transmission through space is called "radiation".[101] Satellites are capable of communicating with more than one earthstation at once, which complicate the legal jurisdictional issue. Most satellites are pure transmission equipment given nicknames like bent-pipe satellites, "minors in the sky," or "microwave towers in the sky." However, there also exist satellites with onboard processing, which have considerably more complicated communications systems because they manipulate the signal going through the transponder. Thus, they do more than simply rebroadcast a signal and may provide for demodulation and remodulation, signal routing and switching, and other functions – so-called "switchboard-in-the-sky." Additional, some high-speed data satellites designed for Internet traffic will have complex data handling and switching abilities – so-called "Internet in the sky."[102] This further complicates the legal jurisdictional issue.

Among satellite-delivered telecommunications applications exist:

- Fixed Satellite Service (FSS), which is intended for communication through a satellite between earthstations that are fixed, or which are within a specified area.
- Mobile Satellite Service (MSS), which is satellite-delivered services to users on the go.[103]

The latter type creates even more legal jurisdictional headaches as it – compared to landlines – makes it more difficult to predict the earthly place of where the end-user is located, since one satellite can re-route a signal to another satellite. Thus, make it possible for a person in the reach of a satellite on the other site of the Earth to catch the data to a mobile internet-receiving unit.

Anyone can upload a satellite,[104] and the trend has been away from governmentally controlled entities owing the satellites and toward privately

[100] CHARTRAND *supra* note 95, at 7. Satellites are left to specialize in the huge (but more diffuse) markets of medium- and thin-density routes, preeminently in mobile communication.

[101] *Id. 77.* Satellites that utilize two different frequency bands are called hybrid satellites.

[102] *Id*. section 13.

[103] *Id*. section 2.6.2.3.

[104] The only restriction is that they must not interfere with satellites in the Clarke Orbit, see below, footnote 92 above and footnote 42-43 in chapter one section 1.6.

owned by multinational corporations.[105] Thus, satellites, whose signals can be received by one State's citizens, can have been uploaded by a private entity located in another State and thereby out of the first mentioned State's jurisdiction. As for communication via satellites under public international law, a State has only the right to make legalization over the operation of Earth stations on its own territory and their communication with satellites. However, telecommunications have significantly diluted the concept of totally independent, sovereign nations. The two simple facts that one cannot stop a radio wave at a national border, and that a single geostationary satellite can see 44 % of the entire surface of the planet, mean that even nations wishing to cut themselves off from others find it impossible to do so completely.[106] Public international law does not allow a State[107] to legislate or make enforcement on satellites and the telecommunication that is offered by a certain satellite.[108]

The State where the owner of a satellite is located or incorporated can of cause give binding orders[109] to that owner as being within its territory or a national.[110] As for satellites in the Geostationary Earth Orbit or Clarke Orbit, the International Telecommunication Union has tried to register satellites (to

[105] *Id.* section 21.

[106] CHARTRAND *supra* note 95, at 12.

[107] The State where the owner of a satellite is located or incorporated can of cause give binding orders to that owner as being within its territory or a national.

[108] BROWNLIE *supra* note 34, at 256-57.

[109] SPANG-HANSSEN *supra* note 15, at 244-252 and JORDAN J. PAUST, INTERNATIONAL CRIMINAL LAW 123 (Carolina Academic Press 1996 – ISBN 0-89089-894-4) [hereinafter JORDAN J. PAUST] (Subjective territorial jurisdiction exists where acts are initiated in or, as is often the case, nearly all the events relevant to a particular case occur within the territorial confines of a State or on vessels, aircraft, spacecraft, or space station subject to its "flag" jurisdiction). In the U.S. the Satellite Division, International Bureau of the Federal Communications Commission issues orders on Space Stations, see for example order DA 03-4095 of 23 December 2003, SAT-WAV-20031202-00352 S2474 and order DA05-50 of 10 January 2006, SAT-AMD-20040227-00021.

[110] As several persons from different countries together can own a satellite and the primary aim for treaties on the outer space is to allow all, on equal terms, to use the outer space, it seems that as far as a common owned satellite in outer space is concerned, that a state only can require of a part-owner, which is one of it's residents or nationals, that the part-owner obey rules, which can be regarded as a common denominator, not a union of the national rules of the co-owners.

prevent collisions in the limited Clarke Orbit at 35,768 km in altitude over Equator and of only 265,000 km of length[111]) by allocating a certain "spectrum" to the different counties in the world. However, not all States has accepted this registration-system.[112] In 1974 the U.N. General Assembly adopted[113] the Convention on Registration of Objects Launched into Outer Space.[114] Article 6 provides that states parties to the Treaty shall bear responsibility for national activities in space, whether such activities are carried on by governmental agencies or by non-governmental entities. Article 4 forbids to place in orbit any object carrying any kind of weapons of mass destruction.[115] However, it should as for public international law be noted, that although registration is much concerned with jurisdiction and control, these are the consequence of specific provisions or practice and not derived from the concept of nationality as for instance with ships and aircrafts.[116]

> Article 6 of the Outer Space Treaty[117] require state parties to the Outer Space Treaty to do continuing supervision of activities of non-governmental entities in outer space.
> Article 7 provides that each State party from whose territory or facility an object is launched[118] is internationally liable for damage to another State party to

[111] KENNEDY *supra* note 93, at 57, 65 and CHARTRAND *supra* note 95, at section 4 and 10.2.

[112] For example China and Kingdom of Tonga, see KENNEDY *supra* note 93, at 57.

[113] Resolution 3235 (XXIX).

[114] 1023 U.N.T.S. 15, reprinted in UNITED NATIONS TREATIES AND PRINCIPLES ON OUTER SPACE 22 (2002 - ISBN 92-1-100900-6) at <http://www.unoosa.org/pdf/publications/STSPACE11E.pdf>. As of May 2006 it has 25 signatories and 48 parties (into force 15 September 1976) <http://untreaty.un.org/ENGLISH/bible/englishinternetbible/partI/chapterXXIV/treaty 1.asp> (visited May 2006). The Convention also applies to any international intergovernmental organization, who accept the Convention and a majority of the States members of the organization are States Parties to the Convention and the Outer Space Treaty.

[115] Article 7 of the Outer Space Treaty assumes that an object launched into outer space will have been registered, and provides that the state of registration will retain jurisdiction and control, OPPENHEIM *supra* note 44, at 833.

[116] OPPENHEIM *supra* note 44, at 834.

[117] See above footnote 87.

> the Treaty or to its natural or judicial persons by such objects or its component parts on the Earth, in air space or in outer space.
> Article 8 provides that a State party to the Treaty on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object…while in outer space. Ownership of objects launched into outer space is not affected by their presence in outer space or by their return to the Earth. Such objects found beyond the limits of the State party to the Treaty on whose registry they are carried shall be returned to that State party, which shall, upon request, furnish identifying data prior to their return.
>
> Article 1 of the Convention on registration of Objects Launched into Outer Space (Resolution 3235 (XXIX) annex) require: When a space object is launched into Earth orbit or beyond, the launching State shall register the space object.

7.6. The Cybercrime Convention of 23 November 2001

The by some people called "Budapest Convention,"[119] which came into force on 1 July 2004, has as of 18 May 2006 42 signatures[120] and 13 parties.[121] Its goal is to "pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation[122] and fostering international co-operation."[123]

[118] "launching state": A state which launches or procures the launching of a space object and a State from whose territory or facility a space object is launched, Convention on International Liability for Damage Caused by Space Objects of 29 March 1972, resolution 2777 (XXVI), annex.

[119] See *supra* note 2.

[120] Cybercrime Convention *supra* note 2.

[121] Albania, Bulgaria, Croatia, Cyprus, Denmark, Estonia, France, Hungary, Lithuania, Romania, Slovenia, the former Yugoslav Republic of Macedonia and Ukraine.

[122] A Global Survey of Cybercrime Laws with translation into English is available at Cybercrimelaw.net (a global information clearinghouse on cybercrime law, edited by Council of Europe expert on cybercrime & Chief Judge Stein Schjølberg, Norway) at <http://www.cybercrimelaw.net/laws/survey.html >. See also WORLD FACTBOOK OF CRIMINAL JUSTICE SYSTEMS (covering 45 countries), at <http://www.ojp.usdoj.gov/bjs/abstract/wfcj.htm> (visited May 2006).

The preamble to the convention states that the "aim of the Council of Europe is to achieve a greater unity between its members" and "fostering co-operation with the other States parties to this convention."[124]

It is mindful "of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data…and takes into account the existing Council of Europe conventions on co-operation in the penal field."

Furthermore, it is "[m]indful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy."[125]

[123] See also EXPLANATORY REPORT OF 8 NOVEMBER 2001 to the convention adopted by the Committee of Ministers of the Council of Europe para 16 [hereinafter CONVENTION-REPORT], at <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (visited December 2005).

[124] President Bush has on 17 November 2003 recommended the Convention to the U.S. Senate enclosed Letter of Submittal from the State Department, S. Treaty doc. 108-11 at <http://www.usdoj.gov/criminal/cybercrime/senateMemo.pdf> and the Senate's Committee on Foreign Relations held a hearing on 17 June 2004 and has on 8 November 2005 issued a report on "Treaty Doc. 108-11" containing a resolution of advice and consent to ratification with 6 reservations and 5 declarations, at <http://www.washingtonwatchdog.org/rtk/documents/cong_reports/executive/109/executivereport109_006.html> (visited November 2005).

[125] Ensuring the protection of fundamental rights to privacy, protection against self-incrimination and unwarranted searches and seizures, and due process of law is critical. Such protections should be prominent among the design criteria for technological, policy, and legal measures, and should be enforced by law and strong economic and political incentives. Governments value liberty, privacy, and security differently, Ekaterina A. Drozdova, *Civil Liberties and Security in Cyberspace in* SOFAER *supra*

A Protocol[126] to the convention was made on 28 January 2003 related to acts of a racist and xenophobic[127] nature, but not intended to affect established principles relating to freedom of expression in national legal systems.[128] As of 18 May 2006 it has 30 signatures[129] and 6 parties.[130] It came into force on 1 March 2006 and refers as for jurisdiction to article 22 of the Convention.

An Explanatory Report[131] to the Convention remarks that "[b]y connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse" and that the "transborder character of such offences, e.g. when committed through the Internet, is in conflict with the

note 3, at 220. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/183.pdf >.

[126] Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems [hereinafter Additional Protocol], at <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.

[127] "racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, article 2 of the Protocol. See also paras 1 and 10-22 in Explanatory Report to the protocol [hereinafter PROTOCOL-REPORT], at <http://convention.coe.int/Treaty/en/Reports/Html/189.htm>.

[128] It also takes into account relevant international instruments, in particular: the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination (consolidated version at <www.echr.coe.int>), the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia.

[129] <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=12&DF=5/18/2006&CL=ENG>.

[130] Albania, Cyprus, Denmark, France, Slovenia, the former Yugoslav Republic of Macedonia.

[131] PROTOCOL-REPORT *supra* note 127, paras 8-9.

territoriality of national law enforcement authorities." The report admits that "[g]iven the cross-border nature of information networks, a concerted international effort is needed."

7.6.1. Crimes under the Cybercrime Convention

The convention divides the types of cybercrimes into 4 categories and articles:[132]

[132] The Cybercrime Convention have created coverage on some issues that is undesirably broad, Abraham D. Sofaer, *Toward an international Convention on Cyber Security in* SOFAER *supra* note 3, at 228. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf >. The STANFORD-PROPOSAL *supra* note 3, suggests in article 3 the following offences: Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent: (a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention; (b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property; (c) enters into a cyber system for which access is restricted in a conspicuous and unambiguous manner; (d) interferes with tamper-detection or authentication mechanisms; (e) manufactures, sells, uses, posts, or otherwise distributes any device or program intended for the purpose of committing any conduct prohibited by Articles 3 and 4 of this Convention; (f) uses a cyber system as a material factor in committing an act made unlawful or prohibited by any of the following treaties: (i) Convention on Offenses and Certain Other Acts Committed on Board Aircraft, September 14, 1963, 20 U.S.T. 2941; (ii) Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking), December 16, 1970, 22 U.S.T. 1641; (iii) Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), September 23, 1971, 24 U.S.T. 564; (iv) International Convention Against the Taking of Hostages, December 17, 1979, T.I.A.S. 11081 [Hostages Convention]; (v) International Convention for the Suppression of Terrorist Bombings, December 15, 1997, 37 I.L.M. 249; (vi) United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, December 20, 1988, T.IA.S., 20 I.L.M. 493; (vii) International Maritime Organization Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, March 10, 1988, IMO Doc. SUA/CON/15/Rev.1, 1993 Can. T.S. No. 10.; (g) engages in any conduct prohibited

- Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems:[133]
  - Article 2 - Illegal access
  - Article 3 - Illegal interception
  - Article 4 - Data interference
  - Article 5 - System interference
  - Article 6 - Misuse of devices
- Title 2 - Computer-related offences:[134]
  - Article 7 - Computer-related forgery
  - Article 8 - Computer-related fraud
- Title 3 - Content-related offences:[135]
  - Article 9 - Offences related to child pornography.
- Title 4 - Offences related to infringements of copyright and related rights:[136]
  - Article 10 - Offences related to infringements of copyright and related rights

Article 11 subsection 1 requires each party to adopt national legislation so it is a criminal offence to intentionally aide or abet the commission of any of the offences in article 2-10. Subsection 2 require the same for an intentionally

under Articles 3 and 4 of this Convention with a purpose of targeting the critical infrastructure of any State Party.

[133] CONVENTION-REPORT *supra* note 123, at paras 35 and 43-78.

[134] CONVENTION-REPORT *supra* note 123, at paras 35 and 79-90.

[135] CONVENTION-REPORT *supra* note 123, at paras 35 and 91-106. Denmark has made reservations to Article 9, see below Appendix 9.

[136] CONVENTION-REPORT *supra* note 123, at paras 35 and 107-117. The convention does not deal with "cybersquatting": (a) deliberate, bad faith abusive registration of a domain name in violation of rights in trademarks and service marks; (b) the practice of registering a collection ("warehousing") of domain names corresponding to trademarks with the intention of selling the registrations to the owners of the trademarks. (c) "cyberpiracy" relating to violation of copyright in the content of websites. WIPO only define (a) as cybersquatting, para 170 OF THE MANAGEMENT OF INTERNET NAMES AND ADDRESSES: INTELLECTUAL PROPERTY ISSUES - FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS 30 April 1999 at <http://arbiter.wipo.int/processes/process1/report/finalreport.html> (visited May 2006).

attempt to commit any offence in article 2-10, except for article 2, 6, 9(1)(b, d-e) and 10, unless the party has made a reservation to subsection 2.

> Article 21 (1)(a) require each party to adopt legislation and other measures in relation to "a range of serious offences to be determined by domestic law"[137] to allow its authorities to collect or record through the application of technical means on the territory of that Party. – This probably allows the party to collect or record content on servers in its territory even though the users of the server is located in another country, where the stored content is legal.
>
> That means each party[138] has to define what is a "serious offence".[139] Safeguards in articles 14 and 15 has to be respected.[140]

None of these crimes classify under public international law to such "serious offences" that allow the use of universal jurisdiction. As "global jurisdiction" is not allowed under public international law, see above chapter 3 sec-

[137] That means each party has to define what is a "serious offence", CONVENTION-REPORT *supra* note 123, para 214. Safeguards are given in articles 14 and 15, para 215.

[138] CONVENTION-REPORT *supra* note 123, para 214.

[139] For example: "*Cybertorts*": refers to the commission of a tortious act, such as defaming an individual, during the process of computer-based communication; "*Cybersmuts*": refers to the process of sending and receiving through computer-based communication material that is defined as obscene or indecent; and "*Cyberracism*": e.g. the Canadian Criminal Code, R.S.C. 1985, c. C-46, § 319(2) (1985)(Every one who, by communicating statements, other than in private conversation, wilfully promotes hatred against any identifiable group is guilty of (a) an indictable offence and is liable to imprisonment for a term not exceeding two years; or (b) an offence punishable on summary conviction) and German Criminal Code § 130. The latter prohibits expressive attacks that incite hatred and Section 131 proscribes the production and dissemination of hate speech. In Germany several provisions of the criminal code are directed at expressions that are inconsistent with the "dignity of the human personality developing freely within the social community," a right that has its basis in Article 1 of the German Constitution. Many other countries have similar laws, Adeno Addis, *The Thin State in Thick Globalism: Sovereignty in the Information Age*, 37 Vand. J. Trans-nat'l L. 1, footnote 149-150 (2004). See also Canadian case *R. v. Keegstra*, CarswellAlta 192, 77 Alta. L.R. (2d) 193, 1 C.R. (4th) 129, [1991] 2 W.W.R. 1, 61 C.C.C. (3d) 1, 117 N.R. 1, 114 A.R. 81, 3 C.R.R. (2d) 193, [1990] 3 S.C.R. 697 (Supreme Court of Canada, December 1990).

[140] CONVENTION-REPORT *supra* note 123, para 215.

tion 3.3.1, the convention's rules on jurisdiction has to be scrutinized as to what extent they are exterritorial (outside the group of countries that are parties to the convention).

The Additional Protocol adds the following as cybercrimes:[141]

- Dissemination of racist and xenophobic material through computer systems
- Racist and xenophobic motivated threat
- Racist and xenophobic motivated insult
- Denial, gross minimisation, approval or justification of genocide or crimes against humanity

This Additional protocol on hate speech probably violates several constitutions rules on free speech[142] and maybe the freedom of speech and expression in the U.N. Declaration on Human Rights.

It also seem to be in conflict with the Convention's article 15[143] that require each party secure adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights

[141] Additional Protocol *supra* note 126, article 3-6. On definition of "racist and xenophobic material", see *id.*article 2. Denmark has reserved the right to fully or to partially refrain from criminalising acts covered by Article 3 (on Dissemination of racist and xenophobic material through computer systems), paragraph 1, Article 5 (on Racist and xenophobic motivated insult), paragraph 1, and Article 6 (on Denial, gross minimisation, approval or justification of genocide or crimes against humanity), paragraph 1, see below Appendix 9. France has declared to article 6 when ratifying that "France interprets the terms "international court established by relevant international instruments and whose jurisdiction is recognised by that Party" (Article 6, paragraph 1) as being any international criminal jurisdiction explicitely recognised as such by the French authorities and established under its domestic law, <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=189&CM=11&DF=7/25/2006&CL=ENG&VL=1> (visited 24 July 2006).

[142] Pursuant to article 8 of the Protocol. See also van Blarcum, *Internet Hate Speech: The European Framework and the Emerging American Haven*, 62 Wash. & Lee L. Rev. 781 (2005).

[143] On some common minimum safeguards, see paras 145-148 in the CONVENTION-REPORT, *supra* note 123.

instruments, and which shall incorporate the principle of proportionality.

Countries outside Europe should probably make reservations if signing the Cybercrime convention as far as they are not parties and thus bound by the European Convention for the Protection of Human Rights and fundamental Freedoms.[144]

The 2006 Danish Cartoon issue is an excellent example of how different cultures and religions interpretate free speech and freedom of the press. The drafters of the Additional protocol should rather have incorporated the main technical principle of the (worldwide) Internet Protocol, namely the "Robustness Principle": "Be liberal in what you accept, and conservative in what you send."[145] Furthermore, the drafters should have taken the wisdom from two American court decisions that involved a large degree of computer technical experts. Namely, the U.S. Federal Court of Appeals for the Third Circuit quoting the U.S. Supreme Court stating that "People in different States vary in their tastes and attitudes and this diversity is not to be strangled by the absolutism of imposed uniformity."[146]

The drafters of the Additional protocol would probably if they had consulted computer technicians behind the Internet Protocol have realized that the Additional protocol is European narrow-minded and that the proper way to solve the European schism was to make a European Firewall like the Chinese and prevent Europeans from getting access to websites that States in Europe don't want their citizens to see, for example the Swastika that is more than legal in Asia where one country uses it as symbol for Red Cross.

The existence of Additional protocol is more than likely in some future

[144] See also Article 39(3) of the Cybercrime Convention *supra* note 2: Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party. This must include public international law.

[145] Request for Comments (RFC) 1122 at 26 <http://ietf.org/rfc.html>. Denmark has when ratifying the Additional Protocol to the Cybercrime Convention reserved the right to fully or to partially refrain from criminalising acts covered by Article 3 (on Dissemination of racist and xenophobic material through computer systems), paragraph 1, Article 5 (on Racist and xenophobic motivated insult), paragraph 1 and Article 6 (on Denial, gross minimisation, approval or justification of genocide or crimes against humanity), paragraph 1, see below Appendix 9.

[146] *ACLU v. Reno*, 217 F.3d 162, 178 (3rd Cir. 2000) *quoting Miller v. State of Californi*a, 413 U.S. 15, 33 (U.S. (Cal), 1973).

when Israel and a Arabic country has ratified the protocol to forbid a lot of information on Judaism and Islam, because either Israel or the Arabic state Party of the protocol will determine the content unsuitable and require it forbidden and violators sentenced.

There is far more sense in following the U.S. Supreme Court that more than once has emphasized that the Internet is a international system and rejected in Reno-2 to apply a "community standards" criterion to the Internet, because it would mean "that any communication available to a nation-wide audience [would] be judged by the standards of the community most likely to be offended by the message."[147]

Thus, if you don't like what is on the Internet, don't hook up or logon. A technical solution is simple. Only hook up through an ISP that censor everything and filter out what you don't like, for example information on Salman Rushdie.[148] Shall the Pope and the Holy See be allowed to censor what should be acceptable content? These would most likely remove all information on contraception and abortion given by U.N.'s World Health Organization or to require extradited the author and persons involved in the Da Vinci Code movie to the Vatican for imprisonment in Castel Sant'Angelo for heresy!

It would have been much wiser of the drafters of the Additional Protocol to advice States to sent all violation to the European Court on Human Rights respectively the American Court of Human Rights. The Additional Protocol is a thoughtless wrongdoing of the Council of Europe and can be expected to overruled by international courts like the European Court on Human Rights respectively the American Court of Human Rights as the protocol imply much more censorship than allowed by customary international law and several treaties. The U.S. has most wisely rejected to ratify the Protocol of First

[147] *ACLU v. Reno*, 217 F.3d at 167 and U.S. Supreme Court in *Reno v. ACLU*, 521 U.S. at 877-878.

[148] <http://en.wikipedia.org/wiki/The_Satanic_Verses> On 14 February 1989, Iran issued a fatwa calling on all Muslims to kill Rushdie for writing the controversial novel The Satanic Verses. The Rushdie fatwa still stands, Iran Focus, 14 February 2006 <http://www.iranfocus.com/modules/news/article.php?storyid=5768> (visited May 2006).

Amendment reasons.[149]

7.6.2. Jurisdiction under the Convention

Article 22 of the convention states as for jurisdiction:[150]

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance

[149] The protocol will not be ratified by the U.S. as it would be unconstitutional because of U.S. Constitution First Amendment's guarantee of freedom of expression, Declan McCullagh, *First 'cybercrime' treaty advances in Senate*, CNET News.Com 26 July 2005 at <http://news.com.com/2100-7348_3-5805561.html> and <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QE1> (visited May 2006). One of the drafters, Henrik W. K. Kaspersen, Professor and Director, Computer/Law Institute, Free University of Amsterdam, stated on 8 March 2002 at a conference at a CyberCrime seminar held by Nordic Association of Law and Edp in corporation with Norwegian Center for Computers and Law, University of Oslo that that the U.S. must give up its some of its protection under the First Amendment when it comes to information on the Internet as the Cybercrime convention otherwise will not work to the extent it was supposed. However, a Californian Appeal Court has recently stated that the First Amendment also apply for the Internet, *Jason O'Grady v. Superior Court of Santa Clara County* (Apple Computer), 44 Cal.Rptr.3d 72, 2006 WL 1452685 (Cal.App. 6 Dist., May 26, 2006 - No. H028579), at <http://www.courtinfo.ca.gov/opinions/documents/H028579.PDF>.

[150] The United States will probably "pursuant to Articles 22 and 42, reserves the right not to apply in part paragraphs (1)(b), (c) and (d) of Article 22 ("Jurisdiction"). The United States does not provide for plenary jurisdiction over offenses that are committed outside its territory by its citizens or on board ships flying its flag or aircraft registered under its laws. However, United States law does provide for jurisdiction over a number of offenses to be established under the Convention that are committed abroad by United States nationals in circumstances implicating particular federal interests, as well as over a number of such offenses committed on board United States-flagged ships or aircraft registered under United States law. Accordingly, the United States will implement paragraphs (1)(b), (c) and (d) to the extent provided for under its federal law," Senate Committee Report Part VII, section 2(2), at <http://www.washingtonwatchdog.org/rtk/documents/cong_reports/executive/109/executivereport109_006.html>. See also Letter of Submittal from the State Department, S. Treaty doc. 108-11 p. xvi-xv at <http://www.usdoj.gov/criminal/cybercrime/senateMemo.pdf> (visited May 2006).

with Articles 2 through 11 of this Convention, when the offence is committed:[151]

(a) in its territory;[152] or
(b) on board a ship[153] flying the flag of that Party; or
(c) on board an aircraft registered under the laws of that Party; or

> Article 22 litra a-c is covering what some call the "territorial sovereignty".[154] As far as the subjective territoriality principle (acts originated in within the territory) is used, there does not seem to be any problems.
> However to the extent that a State wants to use the objective territoriality principle (acts originated abroad) as basis for its exercise of jurisdiction, pub-

[151] The STANFORD-PROPOSAL *supra* note 3, which recognized cyber crime is quintessentially transnational and thus involves jurisdictional assertions of multiple states, tries to avoid this conflict by limiting to cyber activities that are universally condemned. Abraham d. Sofaer, *Toward an international Convention on Cyber Security in* SOFAER *supra* note 3, at 233. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf >. Its suggestion for a rule on jurisdiction is Article 5: 1. Each State Party to this Convention shall take such measures as may be necessary to establish its jurisdiction over the offenses set forth in Articles 3 and 4 in the following cases: (a) when the offense is committed in the territory of that State or on board a ship, aircraft, or satellite registered in that State or in any other place under its jurisdiction as recognized by international law; (b) when the alleged offender is a national of that State; (c) when the alleged offender is a stateless person whose primary residence is in its territory; (d) when the alleged offender is present in its territory and it does not extradite such person pursuant to this Convention.

[152] SPANG-HANSSEN *supra* note 15, at 245-250. ANTONIO CASSESE *supra* note 34, at 277.

[153] As crime and ships should be noted that the *S.S. Lotus* case (France v. Turkey), 1927 P.C.I.J. (Ser. A) No. 10 p. 28, today only has limited value as precedence, because the Convention on the Law of the Sea has made a rule that is opposite to the Lotus ruling. The Lotus decision is in most respect unhelpful in its approach to the principles of jurisdiction, and its pronouncements are characterized by vagueness and generality. This most criticized P.C.I.J. decision has on the issue of state discretion been contradicted by the I.C.J. in the *Anglo-Norwegian Fisheries* (1951 I.C.J. 116, 180) and *Nottebohm* (1955 I.C.J. 4, 411) cases, Brownlie *supra* note 34, at 301, SPANG-HANSSEN *supra* note 15, at 239.

[154] SPANG-HANSSEN *supra* note 15, at 210, BROWNLIE *supra* note 34, at 105, I. A. SHEARER, STAKE'S INTERNATIONAL LAW 185 (11th Ed., Butterworth 1994).

lic international law drawn limits on this principle and its use has been controversy.[155]
The latter seems to be neglected by the Convention-Report that as an example that a party can assert territorial jurisdiction "where the computer system attacked is within its territory, even if the attacker is not".[156] However this example is in violation with public international law.

The main problem with litra a-c is that the convention does not determine when something related to Cyberspace is occurring "in" or "on" the territory. As the computer technology is new, public international law has not developed any practice on when a Cyberspace-act is occurring "in" or "on" the territory.
It should be noted that the drafting committee seems to have neglected specified issue of task no. v (the question of jurisdiction in relation to information technology offences), namely "determine the place where the offence was committed (*locus delicti*)".[157]
This is probably the most difficult and most controversial issue in Cyberspace law, which should have been solved by the drafting committee as the steppingstone before drafting any other articles. See on this subject Spang-Hanssen supra note 15, at 296-462, chapters 31-33.

The convention does not establish jurisdiction over offences involving satellites registered in it name, as the drafters found a provision was unnecessary since unlawful communications involving satellites will invariably originate from and/or be received on earth. The drafters questioned whether registration was an appropriate basis for asserting criminal jurisdiction since in many cases there would be no meaningful nexus between the offence committed and the State of registry because a satellite serves as a mere conduit for a transmission.[158] However, there do exists satellites that are more than "pure" transmission units, see above section 7.5. It can fairly well be expected in near future (caused by the use of wireless devices) that content on a satellite will only be stored in the air but not on a server on earth. Storage on satellites might also be offered free to cybernauts around the world after the same concept as Yahoo has done on Earth, namely advertising revenue.

[155] SPANG-HANSSEN *supra* note 15, at 247-250.
[156] CONVENTION-REPORT *supra* note 123, para 233.
[157] CONVENTION-REPORT *supra* note 123, para 11 subsection v.
[158] CONVENTION-REPORT *supra* note 123, para 234.

As both litra b and c, and the Convention-Report[159] is silent about these two "territories", these subsections must be interpretated pursuant to public customary law, which has been codified into as for ships the Convention on the Law of the Sea,[160] and as for aircrafts the Chicago Convention.[161]
However, the Convention-Report does point out that cybercrimes committed aboard a ship or aircraft only gives jurisdiction to the State of registry. Thus, the convention distinguishes cybercrimes from other crimes and excludes cyber crimes from the regime given for transit passage for ships and aircrafts pursuant to article 42 of the Law of the Sea.

Article 18(1) requires each party to adopt legislation so its authorities can order: (a) a person in its territory to submit specified computer data in that person's possession or control[162], which is stored in a computer system or a computer-data storage medium; and (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.[163]

[159] CONVENTION-REPORT *supra* note 123, para 235.

[160] Convention on the Law of the Sea of 1982 (Montego Bay Convention), U.N. Doc. A/CONF. 62/122, which has 135 parties, and its predecessor, the Convention on the High Seas of 1958, 13 U.S.T. 2312, T.I.A.S. 5200, 450 U.N.T.S. 82, Art. 15. As of May 2006, which has 62 states as parties.

[161] Convention on International Civil Aviation (Chicago Convention) of 7 December 1944, which has 189 parties, at <http://www.icao.int/icaonet/dcs/7300_8ed.pdf> and status at <http://www.icao.int/icao/en/leb/chicago.pdf>. The CONVENTION-REPORT *supra* note 123, para 235 mentions cybercrimes committed aboard a ship or aircraft

[162] "possession or control" refers to physical possession of the data concerned in the ordering Party's territory. A mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision, CONVENTION-REPORT *supra* note 123, paras 173-176.

[163] "possession or control" refers to subscriber information in the ser-vice provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory, CONVENTION-REPORT *supra* note 123, paras 173-176. "Subscriber information" is defined in article 18(3), see also CONVENTION-REPORT *supra* note 123, paras 177-183.

Article 19 on search and seizure of stored computer data does not does not address "'transborder search and seizure", whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance.[164] This issue is discussed below at the Chapter on international co-operation. The other computer system or part of it must also be "in the territory".[165]

Article 30: A party can only reject to disclosure data traffic done by a service providers in its territory if: (a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or (b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

(d) by one of its nationals,[166] if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.[167]

Pursuant to the commentary in Convention-Report[168] to article 22 litra d does the convention only allow jurisdiction based on the Active personality principle (based on the nationality of the suspect). Thus, the convention does not allow the use of the in public international law generally rejected Passive personality principle (based on the nationality of the victim).[169]

Furthermore, the formulation of article 22 litra d limits the normal reach of the Active personality principle as the convention for the principle's use in relation to Cybercrime requires that the (α) "offence is punishable under crimi-

[164] CONVENTION-REPORT *supra* note 123, para 195. See also paras 240-302.
[165] CONVENTION-REPORT *supra* note 123, para 193.
[166] SPANG-HANSSEN *supra* note 15, at 250-252. ANTONIO CASSESE *supra* note 34, at 281.
[167] In a commentary to litra d one of the drafters seems to confuse Universal jurisdiction principle and the content of litra d, as this principle under public international law is not necessary for the State of the offender's nationality, Henrik W.K. Kaspersen, *Jurisdiction in the Cyberspace Convention in* CYBERCRIME AND JURISDICTION - A GLOBAL SURvey 14 (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218) [hereinafter KASPERSEN].
[168] CONVENTION-REPORT *supra* note 123, para 236.
[169] SPANG-HANSSEN *supra* note 15, at 250-252, OPPENHEIM *supra* note 44, at 471-72, BROWNLIE *supra* note 34, at 302 .

nal law where it was committed" or (β)[170] "the offence is committed outside the territorial jurisdiction of any State".
However, as for Cybercrime incident the "α" and "β" limitations have no value whatsoever, since article 22(4) does "not exclude any criminal jurisdiction by a Party in accordance with its domestic law." Thus, the text in litra d beyond requiring the offender to be one if its nationals, is totally superfluous.[171]

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

However, it follows from article 22(3)[172], that no reservation is permitted with respect to the obligation to establish jurisdiction in cases falling under the principle of "*aut dedere aut judicare*".[173]

Furthermore, it follows from article 22(2) that no reservation is permitted with respect to the establishment of territorial jurisdiction under litra a.
However, a party is allowed to make reservations over parts of what is normally under public international law characterized as a the "territorial sovereignty",[174] namely: land territory + territorial sea belonging to the land + seabed and subsoil of the territorial sea + ports + a ship bearing the flag of the state wishing to exercise jurisdiction.

[170] One of the drafters of the convention, Henrik W.K. Kaspersen expect "most parties probably will not implement the second part" of litra d, KASPERSEN *supra* note 167, at 15. See also above footnote 167.

[171] The Convention-Report points out the obvious under public international law on jurisdiction based on nationality, that "to the extent the offence involving a satellite communication is committed by a Party's national outside the territorial jurisdiction of any State, there will be a jurisdictional basis under paragraph 1(d)", CONVENTION-REPORT *supra* note 123, para 234.

[172] CONVENTION-REPORT *supra* note 123, para 237.

[173] The principle of "aut dedere aut judicare" is the duty of the state to extradite or to prosecute the accused; while universal jurisdiction only refer to a right of the state to prosecute the accused, M CHERIF BASSIOUNI AND EDWARD M WISE AUT DEDERE AUT JUDICARE. THE DUTY TO EXTRADITE OR PROSECUTE IN INTERNATIONAL LAW 24 (Martinus Nijhoff Publishers 1995 – ISBN 0792333497).

[174] SPANG-HANSSEN *supra* note 15, at 210, BROWNLIE *supra* note 34, at 105.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

> Jurisdiction established on the basis of paragraph 3 is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested extradition pursuant to the requirements of "Extradition", Article 24, paragraph 6 of this Convention.[175]
>
> Article 24 applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.[176] Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
>
> However, there is no roof over how many years imprisonment the sentence can contain, see below section 7.7.2. on extreme punishment.
>
> This section might present a problem for the United States when considering the reasons for the U.S. not ratifying the ICC-statute (see above footnote77) and the existence of a statute whereby "no agency or entity of the United States government or of any State or local government may extradite any person from the United States to the International Criminal Court, nor support the transfer of any United States citizen or permanent resident alien to the International Criminal Court, 22 U.S.C. 7423 (d).

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

[175] CONVENTION-REPORT *supra* note 123, para 237.
[176] See above footnote 123.

Thus, article 22(4) permits the Parties to establish, in conformity with their domestic law, other types of criminal jurisdiction as well.[177]

This paragraph violates public international law, see below section 7.7.

In July 2006 U.S. federal agents arrested a British citizen and chief executive of London based BetOnSports, who was in the United States on a flight layover. A U.S. court had previous issued a temporary restraning order that prohibited the company from taking bets from United States residents. The British government made offshore gambling companies legal as part of a sweeping Gambling Act passed in 2005. In the U.S. the bettor are not breaking the law, because placing a wzager is legal. If convicted of conspiring to operate an illegal gambling operation the Brite faces up to 20 years imprisonment in the U.S.[178]

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.[179]

In order to avoid duplication of effort, affected Parties are to consult in order to determine the proper venue for prosecution. However, the obligation to consult is not absolute, but is to take place 'where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it

[177] CONVENTION-REPORT *supra* note 123, para 238.

[178] Matt Richtel & Heather Timmons, *The Gambling is Virtual; the Mone is Real*, The New York Times 25 July 2006, at <www.nytimes.com/2006/07/25/business/25gamble.html> (visited July 2006).

[179] As for terrorism one scholar has suggested the following hierarchy for states having concurrent jurisdiction: (1) The state on whose territory the violence actually has an impact (object territorial theory and inapplicable to wholly extraterritorial acts of violence), (2) the state whose security, or important governmental functions or interests are damaged (protective principle), (3) the state of the victims' nationality (passive personality theory), (4) a state on whose territory an element of the offense occurred (subjective territoriality approach), (5) any other state having custody of the accused and the necessary evidence (universality theory). But even if such basis exists, an exorbitant or unreasonable assertion of jurisdiction may be blocked by the "rule of reasonableness", Christopher L. Blakesley, *Jurisdiction as Legal Protection against Terrorism*, 19. Conn. L. Rev. 895, 909-910.

has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation.[180]

Some regard is a failure that the convention does not has a priority.[181]

Article 32(a): A Party may, without the authorization of another Party: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically.

Article 38: Any State may until ratification specify the territory or territories to which the convention shall apply. - But confer with article 22(3).

Article 39(3): Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party – which of cause include public international law. See also Article 15.

7.7. Comments to the Cybercrime Convention

7.7.1. Jurisdiction

A comparative analyze of Cybercrime statutes of numerous States' national laws has been made by others. However, surveys have not analyze whether the national statutes are in violation with public international law, which latter is the decisive.[182] One article[183] seems to claim that there in public in-

[180] CONVENTION-REPORT *supra* note 123, para 239.

[181] Abraham d. Sofaer, *Toward an international Convention on Cyber Security in* SOFAER *supra* note 3, at 233 Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf >.

[182] But, one law review article (see next footnote) seems to claim otherwise by referring to a national supreme court's opinion in *American Banana Company v. United Fruit Company*, 213 U.S. 347, 356 (1909)("the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done"). However, national legislation and court decisions are not sources that the International Court of Justice in the Hague can use, see Article 38 of The Statute for ICJ and SPANG-

ternational law in "the past few decades have [been] seen an expansion in the premises that can support the exercise of criminal jurisdiction."[184] However, it would be more correct to say that national courts in relation to cyberspace issues have tried to claim "Global Jurisdiction", which in overall is not allowed under public international law.[185] The Passive personality principle (also named Passive nationality principle) on Jurisdiction has always been controversial in public international law and has only been recognized in extremely rare, special circumstances, which Cyberspace in general is not.

Furthermore, human rights rules like free speech, no exorbitant imprisonment etc. have come into focus in the last decades and requires States and courts to rethink and change previous priorities.

In addition should be noted, public international law does not use the U.S. division between general and specific jurisdiction.[186] Neither does public international law use the U.S. "minimum test" because what under public international law is relevant, it is not the subjective, political, economic, commercial or social interest, but the objective test of the closeness of connection, of a sufficiently weighty point of contact between the facts and their

HANSSEN *supra* note 15, at 211-214. Furthermore, a State's international right to make legal rules should clearly be distinguished from sovereignty. F.A. Mann firmly rejects a U.S. theory by which "under international law the jurisdiction of a State depends on the interest that State, in view of its nature and purposes, may reasonably have in exercising the particular jurisdiction asserted," F.A. MANN-1 *supra* note 61, at 15 and F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 4 (1990, Clarendon Press, Oxford) [hereinafter MANN-2].

[183] Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cyberspace Jurisdiction*, 4 J. High Tech. L. 1 (2004).

[184] See also *An Introduction in* CYBERCRIME AND JURISDICTION - A GLOBAL SURvey 4 (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218).

[185] See *supra* chapter 3.

[186] SPANG-HANSSEN *supra* note 15, at 261-62. Thus, it is not correct when Susan W. Brenner & Bert-Jaap Koops claims the Cyberspace Convention does not have any "specific" jurisdiction provisions, *supra* note 182, at section III. Furthermore, article 22 (1)(d second part) does contain a specific jurisdiction provision. In addition as for pure online cases, as of the time of writing, no U.S. court has as decided to hold general jurisdiction, see this book chapter 3 section 3.3.4.1.1.

legal assessment.[187] In addition, the U.S. "effect test" is not used.[188] Public international law uses the terms "link" or "closeness" (and reasonableness).[189]

One of the drafters of the Cybercrime convention claims that "under international public law, it is self-evident that a sovereign state is entitled to establish jurisdiction over offences that occur on its territory."[190] However, this statement is only correct so far as a physical tangible thing or a person has been physically hit by a person being inside that State or by a person being an alien (the bullet crosses the border). In other relations it is for the public international society to decide when "an offence occur on its territory" and thus when a state is entitled to establish jurisdiction[191] - especially in "pure online" incidents, see foreword to this book.

Furthermore, he claims that national courts will "assume" no damage is caused in the national territory if the information is in a foreign language or obviously directed to other nationals,[192] and notes that the drafters did not see any need to regulate.[193] However, the receiving user can in his browser have chosen to see only automatic translation of websites. Translations of often used websites can exist on proxy-servers without the knowledge by the alien that made the website in another language than the one the end-user sees. Thus, courts do in practice have no chance to "assume" anything. Furthermore, certain languages are international and courts of countries using such a language can far from "assume" that the information was directed to that country.[194]

The drafters' intention with article 22 was to ensure that parties to the

[187] MANN-2 *supra* note 81, at 12, 15 and MANN-1 *supra* note 61, at 39 & 49.
[188] SPANG-HANSSEN *supra* note 15, at 249, 383.
[189] SPANG-HANSSEN *supra* note 15, at 365, 382.
[190] KASPERSEN *supra* note 167, at 10. He claims it is for the "national law and relating case law" "to determine the *locus delicti* with regard to cybercrimes," *id* at 11.
[191] Including the objective territorial principle, which Henrik W.K. Kaspersen wrongfully calls the "subjective territorial jurisdiction," see *id.* at 12, section 2.2.3.
[192] However, see the *iCraveTV* case mentioned above in Chapter 5, section 5.3.2.2. footnote 63 and Spang-Hanssen *supra* note 15, at Chapter 34, section 34.3.2..
[193] KASPERSEN supra note 167, at 12.
[194] SPANG-HANSSEN *supra* note 15, at 17, 362-63.

convention establish the required level of extraterritorial jurisdiction.[195] However, this is only valid as far as public international law allows it. In addition, as article 22 is worded it is far from obvious that litra a-c (the territorial principle) and litra d (the nationality principle) allow exterritorial jurisdiction.

It would be more correct to say that article 22(4) – besides where the offender is a national, thus embraced by litra d – is in reality a ratifying party's permission to give card blanche to all other parties of the convention as to determine, which cyberspace acts other parties' citizens have to accept as cybercrimes, if the offence is felt (committed) "in" that State's territory, "on' board a ship flying the flag of that party or "on" board an aircraft registered under the laws of that party.

Or stated otherwise, article 22(4) is allowing each party full jurisdiction pursuant to the Objective territoriality principle, which through centuries has been controversy and disputed. No other treaty has ever allowed such a card blanche and the article is probably in violation with several existing treaties and general principles. – For example, that citizens in other States can predict whether they are in violation with the law and that they in overall cannot be penalized for not knowing the law of other States than their own, besides where universal jurisdiction has been allowed by the international society. Compare article 30 of the ICC-statute, which is a codification of customary public international law.

This paragraph totally undermine what in public customary international law and treaties has been a must, namely to reserve state sovereignty and each state's right to determine what is the law for its citizens. The competence of cybernauts' national courts in other party states has been diminished or totally eliminated as far as the right to review a foreign court's decision.

One of the drafters, Henrik W.K. Kaspersen, finds it is perfectly reasonable to prosecute a cybercrime at the beginning of a chain of action by a user

[195] KASPERSEN *supra* note 167, at 10, 13. One then wonders why then article 22 does not deal with satellites. This is probably because he is surprised that under public international law the State of the registrar of a satellite under the subjective territorial jurisdiction has jurisdiction in a similar manner as over ships and aircrafts, see above section 7.5. and that sections footnotes and JORDAN J. PAUST *supra* note 109, at 123. Furthermore, article 22 (1)(d second part) can without any be interpretated to cover satellites.

of an electronic communication network or communication service. However, this is not reasonable to the extent the cybernaut's national penal code contain a provisions that allows an offender to withdraw or discontinue and thereby be free from responsibility.[196]

Most astonishingly, Kaspersen claims that universal jurisdiction under article 22 (1)(d) is allowed to be used "[w]here the satellite is being used for communications between legal subjects on earth."[197] However, universal jurisdiction can only be used where the international society – not a group of parties to a convention – decides this (including that the type of crime is a serious international crime).

He states that article 22 "only regulates inter-Party relations."[198] However this is only true as long as non-parties agree with the parties' interpretation of the "place" where a cyberspace act "occurs". To the extent a non-party disagrees with the parties of the convention and the offender not is a national, then any exercising of territorial jurisdiction will be a regulation of non-party relations as there under public international law is no definition or description of the "place" where a cyberspace act "occur".

Therefore, if the drafters intention was not to interfere with non-parties relations, the consequence must be, that all parties to the convention must decline to exercise jurisdiction whenever a non-party State objects (the alleged offender either is a national of or under public international law has a sufficient close link to the non-party State).

However, on the wording of article 22, does the parties to the Convention gives card blanche to the ratifying parties of the Convention to decide where cyberspace acts occur. Thus, a ratifying state's sovereignty is being limited and its national courts are not allowed to overrule the other State's decision on where the particular cyberspace act occurred as the courts of the parties has to recognize other parties court's decisions. Therefore, other parties having by ratifying the convention achieved exterritorial jurisdiction for it's own courts over other party's nationals, which is thereby deprived the protection of their own state's courts system. This is dangerous as the citizens of con-

[196] See for example § 22 of the Danish Penal Code.
[197] KASPERSEN *supra* note 167, at 13.
[198] KASPERSEN *supra* note 167, at 15.

vention parties in future have to comply with all the other parties different cultural, social and political points of views (put into law), which can be extremely different and strange to the individual cybernaut with his own background.

The most vital mistake in article 22 is that it does not have any definition of what and where a Cyberspace act occurs. Thus, it is in reality allowing exercise of Global jurisdiction. (or "concealed" universal jurisdiction) for the parties' courts. Therefore judges of courts of the parties are allowed to state in relation to article 22 (1)(a-c) that "it is problematic to define and describe the place where a Cyberspace act occurs, but I know it when I see specific facts presented in court."[199]

Kaspersen also claim that that public international law does not protect the alleged perpetrator, because it only regulates the relation between sovereign states.[200] However, the individual have several rights and obligations under public international law and has in the last decades in certain aspects been allowed to have standing.[201] For example, several individuals have been brought before international criminal tribunals (in part since the offender's State did not indict him before a national court), because the individual had violated rights and obligations under public international (humanitarian) law.[202] Also could be pointed out on the principle of favouring the accused

[199] Rewriting of a famous statement given in *Jacobellis v. Ohio*, 378 U.S. 184, 197 (US 1964) (In describing the difficulty in defining obscenity Justice Stewart (concurring) stated: "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it.").

[200] KASPERSEN *supra* note 167, at 15.

[201] *Jurisdiction of the Courts of Danzig Case*, P.C.I.J., Rep. Ser. B., no. 15 (1928) pp. 17-18 (allowing certain individuals to bring action), Article 25 of the European Convention on Human Rights allow individuals to bring petition to the European Commission on Human Rights, F. Malekian, INTERNATIONAL CRIMINAL LAW 40-46 (Borgstrôms Tryckeri AB 1991 – ISBN 91-630-0244-2 & 9) & PARTICULAR EMPHASIS ON THE CONCEPT OF CRIME AND CRIMINAL RESPONSIBILITY 169 (Stockholm 1985), G.I. TUNKIN, THEORY OF INTERNATIONAL LAW 244 (London 1974), BROWNLIE *supra* note 34, at 58, 65, 67 and chapter 25.

[202] *Case against Karadzic* before International Criminal Tribunal for the former Yugoslavia and the *Case against Milosevic*.

and in case of doubt, one should hold for the accused.[203]

In addition, any violations must on its face be predictable, which is part of the reasonableness requirement in public international law. However, the convention try to force alien cybernauts to accept that a foreign court discretionary can determine where the particular cyberspace act occurred and thereby whether the foreign court has territorial – or in essence rather exterritorial - jurisdiction over the alien cybernaut. Compare with the case involving Arnold Schwarzenegger and another American where a British court decided the Internet-defamation has occurred in England.[204]

7.7.2. Dedere aut judicare

The principle of "*aut dedere aut judicare*" - the duty of the state to extradite or to prosecute the accused – must with wording of article 22(3) and article 24 prevents a party from still using the practice accepted by public international law whereby states always have upheld a rights to grant asylum to foreign individuals as an inference from their territorial authority.[205]

But, the aim of the article 24 seems too easy to circumvent and undermine. If extradition is refused by a party that party has an obligation (on the request of the other party) to submit the case "to its competent authorities for the purpose of prosecution". However, this mean that the case might never be brought before a court since the prosecution authority by the convention is not prevented from using its discretion to hold evidence is insufficient "to go to trial." In addition, it is possibility that the prosecutor with the offender "might make a deal" whereby the offender will not be prosecuted but in stead help the prosecution against other offenders.[206] However, the party that was rejected the extradition might far from be satisfied with such an outcome, but

[203] ANTONIO CASSESE *supra* note 34, at 156-57.

[204] Mentioned above in chapter 1 section 1.9, *Anna Richardson v. Arnold Schwarzenegger, Sean Walsh and Sheryl Main* [2004] EWHC 2422 (High Court, Queens Bench Division, October 29 2004 – case no. HQ04X01371). See also, Case Comment: Arnold Schwarzenegger Case not Termi-nated, Entertainment Law Review, Ent. L.R. 2005, 16(6), 156-158. See also the i*CraveTV* case in SPANG-HANSSEN *supra* note 15, at 478-482.

[205] OPPENHEIM *supra* note 44, at 950, and BROWNLIE, *supra* note 34, at 313-14.

[206206] See WORLD FACTBOOK OF CRIMINAL JUSTICE SYSTEMS *supra* note 109.

has been given no means or instrument to secure a court system has the final say about the alleged cybercrime. Thus, the rule *dedere aut judicare*[207]can hardly be stated to be a rule in article 22 (3).[208]

7.7.3. Double jeopardy (ne bis in idem)

Double jeopardy (*ne bis in idem*)[209] is not dealt with in the convention. The drafters of the Cybercrime convention was of the opinion that the principle of double jeopardy (ne bis in idem) does not exists in public international law.

However, scholars that belong to the source-category of ICJ article 38(d) holds that there in public international law is a requirement against "double criminality" in connection to extradition and furthermore, that extradition is only appropriate for more serious offences.[210] Thus, parties to the Cybercrime convention of cause also have an obligation not to violate the principle.[211]

The principle of double Jeopardy (*ne bis in idem*) is enshrined in the major human rights treaties, that is, article 14 of the International Covenant on Civil and Political Rights, article 4 of Protocol 7 of 22 November 1984 to the

[207] The principle of "aut dedere aut judicare" - the duty of the state to extradite or to prosecute the accused, (while universal jurisdiction only refer to the right of the state to prosecute the accused), M CHERIF BASSIOUNI AND EDWARD M WISE AUT DEDERE AUT JUDICARE. THE DUTY TO EXTRADITE OR PROSECUTE IN INTERNATIONAL LAW 24 (Martinus Nijhoff Publishers 1995).

[208] As claimed by KASPERSEN *supra* note 167, at 17. He ads that a party "should" prosecute, which might be an admission that article 3 para 3 does not contain a rule of extradition or prosecution.

[209] The principle of "ne bis in idem" (non bis in idem or non bis idem or double jeopardy)(Not twice for the same thing) - forbidding more than one trial for the same offense.

[210] OPPENHEIM *supra* note 44, at 957-58 and BROWNLIE *supra* note 34, at 313-318. Cassese holds that a customary rule is evolving at least with regard to international crimes, because they involve all States., ANTONIO CASSESE *supra* note 34, at 320-321.

[211] Kaspersen seems to believe that parties of the convention, which does not have extradition treaties and/or laws against double jeopardy, is not bound by the principle, KASPERSEN *supra* note 167, at 22. Brenner and Koops claims that Double jeopardy (*ne bis in idem*) is only barring multiple prosecutions for the same offense by the same sovereign, *The Next Step: Prioritizing Jurisdiction in* CYBERCRIME AND JURISDICTION - A GLOBAL SURVEY 328 (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218).

European Convention on Human Rights.[212] The Human Rights Committee in *A v Italy* took the view that double jeopardy is only prohibited with regard to an offence adjudicated in a given state, but not in a different state.[213] The European Commission on Human Rights in *S v Germany*[214] allowed Germany to convict and sentence applicant upon return to Germany after being sentenced for the same narcotics offence in the Netherlands.

Furthermore, article 54 of the Schengen Treaty of 14 June 1985 prohibits a second trial in any other party to the treaty.[215] Thus, the European countries that are party to the Schengen Treaty is bound to follow chapter 3 and thus the principle written into article 54 which provides: "A person who has been finally judged by a Contracting Party may not be prosecuted by another Contracting Party for the same offences provided that, where he is sentenced, the sentence has been served or is currently being served or can no longer be carried out under the sentencing laws of the Contracting Party."

The Schengen Treaty article 56 further provides, that : [i]f further proceedings are brought by a Contracting Party against a person who has been finally judged for the same offences by another Contracting Party, any period of deprivation of liberty served on the territory of the latter Contracting Party on account of the offences in question must be deducted from any sentence handed down. Account will also be taken, to the extent that national legislation permits, of sentences other than periods of imprisonment already undergone.

There seems to be some confusion about the actual meaning of the prohibition of double jeopardy, partly because some states have statutory procedures which allow a retrial if new evidence is found.[216]

The European Court of Justice has stated on article 54:

[212] Christoph J.M. Safferling, Towards an International Criminal Procedure 319-331 (Oxford University Press 2001 – ISBN 0-19-926450-3) [hereinafter SAFFERLING].

[213] SAFFERLING *supra* note 212, at 320 and *A v Italy*, Human Rights Committee (HRC) Doc A/43/40, 242.

[214] *S v Germany*, European Commission on Human Rights (ECommHR) 13 December 1983 Appl. No. 8945/80, 39 DR, 43.

[215] Confer Schengen Treaty article 55. At <http://www.privacy.org/pi/intl_orgs/schenegan_agreement.txt> (visited May 2006).

[216] SAFFERLING *supra* note 212, at 321.

The principle ne bis in idem enshrined in Article 54 does not fall to be applied to a decision of the judicial authorities of one Member State declaring a case to be closed, after the Public Prosecutor has decided not to pursue the prosecution on the sole ground that criminal proceedings have been started in another Member State against the same defendant and for the same acts, without any determination whatsoever as to the merits of the case.[217]

The ne bis in idem principle enshrined in Article 54 must be applied to criminal proceedings brought in a Contracting State for acts for which a person has already been convicted in another Contracting State even though the Convention was not yet in force in the latter State at the time at which that person was convicted, in so far as the Convention was in force in the Contracting States in question at the time of the assessment, by the court before which the second proceedings were brought, of the conditions of applicability of the ne bis in idem principle. Article 54 of the Convention must be interpreted as meaning that:

- the relevant criterion for the purposes of the application of that article is identity of the material acts, understood as the existence of a set of facts which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected;
- punishable acts consisting of exporting and importing the same narcotic drugs and which are prosecuted in different Contracting States to the Convention are, in principle, to be regarded as 'the same acts' for the purposes of Article 54, the definitive assessment in that respect being the task of the competent national courts.[218]

The ne bis in idem principle, laid down in Article 54 also applies to procedures whereby further prosecution is barred, such as the procedures at issue in the main actions, by which the Public Prosecutor of a Member State discontinues criminal proceedings brought in that State, without the involvement of

[217] Reference for a preliminary ruling from the Tribunale di Bologna (Italy) in the criminal proceedings brought against *Filomeno Mario Miraglia*, 2005 E.C.R I-02009, O.J. C 132 , 28/05/2005 P. 0010 – 0011 (ECJ (Fifth Chamber), 10 March 2005 - Case C-469/03).

[218] Reference for a preliminary ruling from Hof van Cassatie (Belgium) in criminal proceedings against *Leopold Henri Van Esbroeck*,2006 E.C.R 00000 (ECJ (Second Chamber), 9 March 2006 - Case C-436/04).

> a court, once the accused has fulfilled certain obligations and, in particular, has paid a certain sum of money determined by the Public Prosecutor.[219]

7.7.4. Extreme foreign punishment

Under public international law any penalty has to be reasonable and foreseeable. In the online perspective should be noted that some California courts have claimed to have jurisdiction over alien cybernauts because of the large amount of servers and high tech companies in that state.

At this place it therefore seems appropriate to mention that California in 1993 enacted the so-called "Three Strike" rule, which mean a minimum sentence of imprisonment in a state prison for 25 years if a defendant has two or more prior felony convictions (including from another state).[220]

[219] Reference for a preliminary ruling from the Oberlandesgerich Köln (Germany) and Rechtbank van eerste aanleg te Veurne (Belgium) for a preliminary ruling in the criminal proceedings before those courts against *Hüseyin Gözütok* and *Klaus Brügge*, O;J. C 083 , 05/04/2003 P. 0005 – 0005, 2003 E.C.R. I-01345 (ECJ, 11 February 2003 - C-187/01 and C-385/01).

[220] California Penal Code §§ 667 and 1170.12. Other U.S. States have similar rules. For example in 2003 a federal appeals court upheld a "three strikes" sentence of a 26 yar to life for Santos Reyes, whose third strike involved trying in 1998 to take the written portion of a driver's license test for his illiterate cousin. The conviction followed two previous offenses, one for a juvenile burglary conviction in 1981 and another for an adult robbery conviction in 1987, B. Bergmank, *Shortsighted Sentence POLICIES*, CHAMPION May 2006, 30-May Champ 4. See also, *Fausto v Hickman*, 2003 WL 21439215 (N.D. Cal., 9 June 2003 – No. C00-4617 MMC(PR))(It was not grossly disproportionate to the crime, to sentence defendant to 25 years to life under three strike law for possession of .04 grams of heroin). *Ewing v. California*, 538 U.S. 11 (US Supreme Court March 2003)(Third strike sentence of 25 years for shoplifting three golf clubs worth $399 apiece did not violate US Const. 8th Amendment on "cruel and unusual punishment), *Lockyer v. Andrade*, 538 U.S. 63 (US Supreme Court March 2003)(Two counts of shoplifting videotapes worth total $153.54 was under Three strikes rule sentenced to 50 years to life, which was not unreasonable or gross disproportional). An "exceedingly rare" exception is *Ramirez v. Castro*, 365 F.3d 755 (9th Circuit April 2004). WITKIN, CALIFORNIA CRIMINAL LAW Vol. 3, 456 (3rd Ed. 2000) and JENNIFER E. WALSH, TOUGH FOR WHOM?: HOW PROSECUTORS AND JUDGES USE THEIR DISCRETION TO PROMOTE JUSTICES UNDER THE CALIFORNIA THREE-STRIKES LAW (Henry Salvatory Center 2004) at

This rule is probably so rare and offensive for Europe that European governments should take this into consideration before extraditing persons from their territories. Furthermore, use of a "three strike rule" would probably be rejected by the European Court for Human Rights under Article 7, wherefore a European government would be liable if it extradite a cybernaut to a state, which uses a "three strike rule."

> Article 53 (Safeguard for existing human rights) of the Europe Human Rights convention[221] states: "Nothing in this Convention shall be construed as limiting or derogating from any of the human rights and fundamental freedoms which may be ensured under the laws of any High Contracting Party or under any other agreement to which it is a Party."
>
> The European Court of Human Rights stated in *Kokkinakis*[222] that Article 7 of the Convention include the "principle that the criminal law must not be extensively construed to an accused's detriment…This condition is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him liable."

Furthermore, for example courts in the U.S. uses as sentence system, where each penalty is added to another, whereas in Europe many courts in stead make a sentence that is a lump of all the offences.

No cybercrime – except in very rarely and extreme cases – involve any physical injury on another living person, which is usually the requirement for giving a life-sentence in Europe.

> From World Factbook of Criminal Justice Systems[223] can be mentioned:

<http://salvatori.claremontmckenna.edu/publications/pdf/Walshmonograph.pdf> (visited May 2006).

[221] European Convention for the Protection of Human Rights and Fundamental Freedoms, see above footnote 128.

[222] *Kokkinakis v. Greece*, [1993] ECHR 20 para 52 (European Court of Human Rights, 25 May 1993 No 14307/88) and D.J. HARRIS, LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 274 (Butterworths 1995 – ISBN 0-406-25930-5).

[223] (covering 45 countries) at <http://www.ojp.usdoj.gov/bjs/abstract/wfcj.htm> (visited May 2006).

Czech Republic allows only in extraordinary cases penalties such as 15 to 25 years imprisonment or life imprisonment (No death-penalty);
Denmark allows only in extraordinary cases penalties over 16 years (No death-penalty);
England and Wales has for all practical purposes abolished the death penalty. Around 80% of offenders found guilty are fined (of the in 1994 5.3 million recorded notifiable offense);
France only allows the regular Correctional Courts a maximum of 10 years imprisonment. Life imprisonment can only be sentenced by ad hoc courts (No death-penalty).

7.8. Final Remarks

Security and freedom are both important principles for the growth and development of States.[224] However, as one statesman once stated: They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.[225]

Just as part of the Convention is a powerful – and to a certain extent needed – tool for law enforcement, it is a fearful convention for Cybernauts' freedom of speech and freedom of exchange of information.

When remembering the problems and arguments for not reaching a draft to a convention on jurisdiction and enforcement on civil matters, see Spang-Hanssen 453-458,[226] one can wonder why any state dare considering ratifying the Cybercrime Convention.[227] The CyberCrime convention should not have

[224] Council of Europe expert on cybercrime & Chief Judge Stein Schjølberg, and Amanda M. Hubbard, Computer Crime and Intellectual Property Division, U.S. Justice Department, *Harmonizing National Legal Approaches on Cybercrime* 18, WSIS Thematic Meeting on Cybersecurity June 2005, Doc: CYB/04 <http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf> (visited May 2006).

[225] Benjamin Franklin, *Historical Review of Pennsylvania* (1759) <http://www.quotationspage.com/quote/1381.html> (visited May 2006).

[226] SPANG-HANSSEN *supra* note 15.

[227] As a general principle of international law, a treaty in force is binding upon the parties and must be performed by them in good faith (pacta sunt servanda), codified into arti-

tried to make jurisdiction rules that can give extreme results. It has followed the line of least resistance as for the problems of jurisdiction respectively extraction and made the situation for alien Cybernauts extreme and unpredictable. The reach and impact of the convention should be strictly scrutinized by for example the International Law Commission.

As far as information stored on a satellite the cybernaut does not have to worry, as the Cybercrime Convention pursuant to the Explanatory Report does not cover information stored in Outer Space.[228]

Those states that ratify give up vital rights for their constituents and the protection of its citizens together with fundamental rights in the U.N. Human Rigths Declaration of 1948 which has been the cornerstone for later drafted treaties and U.N. resolutions.

The Cybercrime convention does not have any minimum age limit for the exercise of exterritorial jurisdiction, which must be regarded as a violation of public international law. It should be remembered that many of the violators of crimes dealt with in the convention are minors, which think it is fun to be a cracker but without any criminal intent to gain profit or participate in Information Warfare (destroy other State's main computer systems). Compare with article 26 in the ICC-statute that codifies customary public international law.[229]

At the same time, many of the provisions in the Convention must be considered daily to be violated by computer personnel in the parties' military that are dealing with Information Warfare. Some parts of articles 2-11 might be related to Cyberspace Warfare, see Spang-Hanssen Chapter 14,[230] and thus be "set aside" by jus cogens rules on the laws of war, where it is generally accepted that breaches of the laws of war may be punished by any state, which obtains custody of persons suspected of responsibility.[231]

cle 26 of the Vienna Convention on the Law of Treaties, *supra* note 68, BROWNLIE *supra* note 34, at 591-597.

[228] CONVENTION-REPORT *supra* note 123, para 234.

[229] See as for the ICC above footnote 79.

[230] SPANG-HANSSEN *supra* note 15, at 110-115 and above section 7.4.

[231] BROWNLIE *supra* note 34, at 303 & 563-566 and OPPENHEIM'S INTERNATIONAL LAW VOL. II ON DISPUTES, WAR AND NEUTRALITY 226-236 & 566-588 (7th Ed. Edited by H. Lauterpacht, Longmans 1952).

The convention does not make any boundaries for what military and law enforcement may do or not do. The convention is totally silence when it comes to controlling authorities for violations of public international law. With the provisions given in the convention it is from a human rights perspective dangerous that the convention does not require the parties to make a controlling body for misuse of surveillance and misuse of data of the parties' authorities.

The convention has to an overwhelming degree been drafted as an legislation for a federal republic or a European Union, where there participating states already has given up large parts of their sovereignty to a federal or interstate organ. However, most of the countries in the world is not part of the European Union and thus not given up any sovereignty. The European Arrest warrant system cannot be transferred without heavy limitation to cover the rest of the world.

> The Convention on Cybercrime will endanger Americans' privacy and civil liberties and place the FBI's massive surveillance apparatus at the disposal of nations with much less respect for individual liberties. U.S. Internet service providers are worried about becoming surveillance arms for despotic regimes.[232]
>
> The Cybercrime Treaty "goes way beyond combating Cybercrime…It would require nations that participate in the treaty to adopt all sorts of intrusive surveillance measures and cooperate with other nations, even when the act that's being investigated is not a crime in their home country."[233]
>
> In February 2006 members of the U.S. Congress proposed legislation to deter foreign companies' from cooperating with Chinese censors.[234]

[232] Declan McCullagh, *Fuzzy logic behind Bush's Cybercrime treaty*, NEWS.COM 28 November 2005 at <http://news.com.com/2010_1071_3-5969719.html> (visited November 2005).

[233] Barry Steinhardt, director of the American Civil Liberty Union's technology and liberty program, to Declan McCullagh, *Bush pushes for Cybercrime treaty*, NEWS.COM 18 November 2005 at <http://news.com.com/Bush+pushes+for+cybercrime+treaty/2100-1028_3-5108854.html> (visited November 2005).

[234] Chris Buckley, *Internet muck-raker challenges China's Censors*, REUTERS 17 February 2006 <http://www.prisonplanet.com/articles/february2006/170206censors.htm> (visited Feb 2006).

> In May 2006 it was revealed that three major telephone companies in September 2001 had turned over records of teens of millions of their customers' phone calls to the U.S. National Security Agency.[235]
>
> In February 2006 the House of Lords restricted Government plans to allow the police to order the take down of suspected terrorism-related web content by further requiring that the authorities obtain the permission of a judge first.[236]
>
> Cybercrime laws have never included laws to control illicit drug trafficking and such a development is not preferable as computer-related crime or Cybercrime traditionally are well defined and should not be mixed up with other categories of crimes.[237]
>
> Stein Schjølberg has suggested that the International Law Commission should work on a proposal for amendments of the Rome Statute of the International Criminal Court to include cyberterrorism and serious cybercrimes.[238]

Since much of the Cybercrime convention deals with electronic data parts of the rules in the convention might be in violation with the E.U. Directive on Data Protection, which prohibit the transfer of personal data to a third country that does not ensure an adequate level of protection.[239] This will be a case to decide for the European Court of Justice, which court in the last couple of years also has taken Human Rights aspects into consideration.

[235] *Report: U.S. Spies on Everyone*, WIRED NEWS 11 May 2006 at <www.wired.com/news/wireservice/1,70878-0.html> (visited May 2006).

[236] *Lords restrict terror website censorship plans*, OUT-LAW.COM 3 February 2006 at <www.out-law.com/page-6602> (visited February 2006).

[237] Council of Europe expert on cybercrime & Chief Judge Stein Schjølberg, *Law Comes to Cyberspace*: A presentation at the 11th UN Criminal Congress, 18-25 April 2005, Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime, <http://www.cybercrimelaw.net/documents/UN_Bangkok_05.htm> (visited May 2006).

[238] *Id.*

[239] 57th recital of Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23/11/1995, p 0031–0050, as amended by Regulation (EC) No 1882/2003 of 29 September 2003, O.J. L 284, 31/10/2003, p 0001–0053.

> In the case *European Parliament v Council of the European Union & Commission of the European Communities*[240] the European Court of Justice held: "Article 3(2) of the Directive excludes from the Directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law...and in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law." As the agreement in dispute stated that Passenger Name Record "data will be used strictly for purposes of preventing and combating terrorism and related crimes, other serious crimes, including organised crime, that are transnational in nature, and flight from warrants or custody for those crimes," the decisions made by Council of the European Union & E.U. Commission has to be annulled.[241]

Even though the convention does not mention it, public international law does require reasonableness for jurisdiction to adjudicate. At present, none of the articles 2-11 can be said to have become customary law and thus does not allow universal jurisdiction.[242] Some parts of article 22 are built on the objec-

[240] *European Parliament v Council of the European Union & Commission of the European Communities*, 2006 E.C.R… (E.C.J. C-317/04 and C-318/04, 30 May 2006) (Plaintiff sought annulment of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of Passenger Name Record of air passengers data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (O.J. L 183 , 20/05/2004 p 0083, and corrigendum at O.J. L 255 , 30/09/2005 p 0168) and annulment of Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (O.J. L 235 , 06/07/2004 p 0011 – 0022).

[241] *Id.* paras 54-55, 61 and 69-70. See further E.U. Commission's two proposals of 19 June 2006 (IP/06/800) at <http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/800&format=HTML&aged=0&language=EN&guiLanguage=en>, Report of 19 July 2006 from the European Parliament's Committee on Civil Liberties (Doc. A6-0252/20006 Final) at <http://www.statewatch.org/news/2006/jul/ep-libe-eu-us-pnr-report.pdf> and page 3-6 in Report of 12 July 2006 from the U.K. House of Commons at <http://www.publications.parliament.uk/pa/cm200506/cmselect/cmeuleg/34-xxxv/34-xxxv.pdf> (visited August 2006).

[242] SPANG-HANSSEN *supra* note 15, at 429-430.

tive territoriality principle,[243] which in many relations have been controversial and opposed by many states.[244] Article 30 of the ICC-statute should be incorporated in the Cybercrime Convention.

The World Summit on the Information Society stated that measures to fight cybercrime must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.[245]

The present text of the convention and its protocol show the lack of technicians participating in the drafting.[246] However, technicians' participation is required and should be invited when consideration of changes to the convention next is on the table, see Henrik's Sixth Base.[247]

As a last remark, I think the convention's part dealing with intensifying states' cooperation of their law enforcement and creating new tools to combat and coordinate cybercrimes as for example child pornography and sexslave-trade should be encourages to the largest extent possible, but the convention's rules on jurisdiction should be abolished.

Finally, the speed with which this convention was drafted and comparing it with the long range of decades it took before making a draft for a convention on the area regarded as the international sea (the High Sea), should make

[243] CONVENTION-REPORT *supra* note 123, para 232. See also, SECURITY AND PRIVACY FOR THE CITIZEN IN POST-SEPTEMBER 11 DIGITAL AGE: A PROSPECTIVE OVERVIEW 30 (European Commission Joint Research Centre July 2003 - EUR 28823 EN) at <http://www.jrc.es/home/publications/publications.cfm?pub=1118> (eur20823en.pdf).

[244] The Report of the Working Group on Internet Governance of June 2005 para 17 states there is a lack of efficient tools and mechanisms to be used by countries to prevent and prosecute crimes committed in other jurisdictions, REPORT FROM THE WORKING GROUP ON INTERNET GOVERNANCE (WGIG) page 6, Doc. WSIS-II/PC-3/DOC/5-E of 3 August 2005 at <www.itu.int/wsis/docs2/pc3/off5.doc> (visited July 2006).

[245] Para 42 of the Tunis Agenda for the Information Society, WSIS OUTCOME DOCUMENTS 77 (International Telecommunication Union, December 2005) at <www.itu.int/wsis/promotional/outcome.pdf> (visited July 2006).

[246] "[T]he management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental international organizations ",Para 35 of the Tunis Agenda for the Information Society, WSIS OUTCOME DOCUMENTS 75 (International Telecommunication Union, December 2005) at <www.itu.int/wsis/promotional/outcome.pdf> (visited July 2006).

[247] *Supra* page 7 and SPANG-HANSSEN *supra* note 15, at 519-522.

states hesitate to ratify the Cybercrime Convention as the Internet is only two decades old and taking into consideration that the computer technology changes nearly every six month, which of cause already has made the convention an ancient – and to certain extent – an outdated document ("Human Trafficking through the Internet is one of the top-three crimes today but not a content-related offence). The states of the world should accept the wisdom of justice Souters' statement: "we should be shy about saying the final word today about what will be accepted as reasonable tomorrow…if we had to decide today…we would get it fundamentally wrong."[248] On basis of this statement States should abstain from ratify the convention as it is present formulated.

[248] *Denver Area Educational Telecommunications Consortium, Inc. v FCC*, 518 U.S. 727, 777 (U.S. 1996).

CHAPTER 8

Certain Danish Criminal Provisions related to Cyberspace

By Henrik Spang-Hanssen

8.1. Introduction

The law of Denmark[1] is part of the family of Nordic law that belongs to Civil Law, although they must undoubtedly be admitted to form a special legal family, alongside the Romanistic and German legal families. Roman law has played a smaller role in the legal development of the Nordic countries than in Germany. Nordic law has few, if any, of the "stylistic" hallmarks of the Common Law.[2] Also, it should be noted that political and cultural ties between the Scandinavian countries have always been very close. Thus, what here is written on Danish Law covers to a certain extent the other Scandinavian countries as well, for example there exists several special conventions between the Scandinavian countries of which some will be mentioned in the following.

Furthermore, it should initially be pointed out that Denmark does not use the Stare Decisis Doctrine and only a modest selection of the cases are published in the Danish Case Reporter (Part A) [hereinafter *UfR*[3]]. Additionally,

[1] See abbreviations in Appendix 10.

[2] ZWEIGERT, K. & H.KOTZ, INTRODUCTION TO COMPARATIVE LAW 277 (Clarendon Press, Oxford 1998, 3rd Edition – Translation by Tony Wier – ISBN 0-19-826859-9) and MICHAEL BOGDAN, KOMPARATIV RÄTTSKUNDSKAP 91-92 (Norstedts Juridik, Sweden, 1993, 1. Ed. ISBN 91-38-50200-3).

[3] See further explanation on citation in Appendix 10.

it should be pointed out that most of the Danish legislation on cybercrime has been changed in the last couple of years. Therefore many old cases are not worth mentioning here.

8.2. National Cybercrime Legislation

In Denmark, cybercrime is named "IT-kriminalitet" or "Datakriminalitet". However, there is no exact definition hereof in the Civil Penal Code[4] and to some extent the terms are used differently in the Civil Penal Code and special legislation. In this chapter, the term "cybercrime" will be used.

As for the question of analogizing from previous statutes to new cybercrimes the principle in Danish law is that penalty only can be issued for a conduct, if a statute declares the conduct a crime, or the conduct can be considered total equal to a statutory crime ("absolute analogy").[5] Furthermore, prohibition of analogizing follows from Article 7.1.1 of the European Human Rights Convention,[6] which Denmark is party of, states: "No one shall be held guilty of any criminal offence on account of any act or omission, which did not constitute a criminal offence under national or international law at the time when it was committed." The practice of the courts in Denmark is ambiguous. In cases such as *Prosecutor v. Gotthards*[7] and *Prosecutor v. T*, UfR

[4] A unofficial translation into English as of 2003 is made by VAGN GREVE, GITTE HØYER, MALENE FRESE JENSEN & MARTIN SPENCER, THE DANISH CRIMINAL CODE & THE DANISH CORRECTIONS ACT (2.Ed 2003, DJØF Publishing - ISBN 87-574-0218-3). A general introduction in English to Danish criminal law is made by LARS BO LANGSTED, PETER GARDE & VAGN GREVE, CRIMINAL LAW DENMARK (2 Ed. DJØF Publishing – ISBN 87-574-1057-7).

[5] Danish Civil Penal Code § 1. The latest consolidated version of the law is printed as no. 909 of 27 September 2005 with amendments by laws no. 1389 of 21/12/2005 and 1400 of 21/12/2005.

[6] Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (Council of Europe, ETS No. 5).

[7] *Prosecutor v. Erik Georg Gotthards et al*., UfR 1940.156 Ø (Court of Appeals for Eastern District, 21 October 1939 – Doc. I 251/1039)(Listening to phone calls by connecting a secret bugging-device).

1996.356 Ø[8] was used an extensive analogy. Opposite in *Prosecutor v. T*, UfR 1990.70 H.[9] It is the overwhelming opinion that clear authority in law has to be preferred, rather than a legislation trying to cover all prospects for future technology.

Pursuant to §21 of the Danish Civil Penal Code conducts, which promotes or leads to a crime, is criminalized as attempt when the offense is not completed. The starting point in Danish law is that ordinarily preliminary actions cannot be regarded as an attempt as crime, unless they have a certain gross or dangerous nature.

A person under §23 of the Danish Civil Penal Code is aiding - and thus a criminal accessory - if the person by incitement or by word and deed has contributed to the crime. The overall principle is that there has to be evidence of a criminal intentional act. Pursuant §2 of the Civil Penal Code, §23 also covers violation in special legislation. However, certain statutes also makes gross negligence a crime, for example violation of §76 of the Danish Copyright Act. The question of aiding has been brought into focus caused by the technicality of the Internet where it often is impossible to determine who has produced or forwarded defamatory information. At this point, it should be pointed out that immunity of Internet Service Providers in the U.S. is broader than the one given in Article 12 of the E.U. Directive on electronic commerce, which covers only pure aiding ("mere conduit").[10]

As for criminal intent, it should be pointed out that it is not sufficient to prove that a person by which a non-activated virus is found, has previously done similar destructive acts. Intent requires proof of acts of further preparation than the pure act of constructing the virus.

[8] *Prosecutor v. T*, UfR 1996.356 Ø (Court of Appeals for Eastern District, 22 November 1995 – Doc. S-1948-95)(Whether a "system based on PC-diskettes could be regarded as pyramid-letters).

[9] *Prosecutor v. T*, UfR 1990.70 H (Supreme Court of Denmark, 24 November 1989)(Whether applications via telex should be regarded as a "document" pursuant to the Civil Penal Code).

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), O.J. L 178 , 17/07/2000 p. 0001 – 0016.

8.2.1. Brief Legislative History

In 1985,[11] the first of a number of offences relating to cybercrime was amended to the Danish Civil Penal Code.[12] As for pornography should at this point be mentioned that by amendment of 1969 to the Civil Penal Code a statute against picture-pornography was abolished. That amongst others had made it illegal to make public or disseminate child pornography. However, making child pornography pictures have always been illegal pursuant to Chapter 24 of the Civil Penal Code, including aiding. In 1994 a new subsection was two added to §235, which deal with crude child pornography. By the amendment of 1996 the criminal statute on written statements was expanded to also cover statements given "through other readable medium."[13]

Different amendments made in Danish law in 2004 allow Denmark to ratify the Cybercrime Convention,[14] which Denmark were signed on 22 April 2003.[15] Ratification was done on 21 June 2005[16] with reservations to Articles 9, 14 and 38 of the Convention[17] and Articles 3, 5, 6 and 14 of the Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.[18]

Major amendments to the Civil Penal Code relating to cyber crime were enacted by law no. 352 of 19 May 2004, which came into force on 1 July 2004. In December of 2004 there was enacted legislation related to enforce-

[11] Law no. 229 of 6 June 1985. See also Danish Recommendation-report 1032/1985 on cyber crime.

[12] Could also be translated: "Civil Criminal Code". Denmark has also a Military Criminal Code.

[13] Law no. 388 of 22. May 1996 concerning Civil Penal Code § 163.

[14] ETS no. 185 of 23 November 2003 ("Budapest Convention").

[15] See section 1.1 of remarks to bill L 55 of 5 November 2003, enacted as law no. 352 of 19 May 2004 (in force 1. July 2004).

[16] Chart of signatures and ratifications, Council of Europe at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=11&DF=22/08/2005&CL=ENG> (visited 22 August 2005).

[17] The Convention does not apply to the Feroe Islands and Greenland, see text of reservations reprinted as Appendix 9.

[18] The Protocol does not apply to the Feroe Islands and Greenland, see text of reservations reprinted as Appendix 9.

ment of decisions from other E.U. Member States and to the Europol Convention.[19] In March 2006 was implemented an E.U. directive on enforcement of intellectual property rights.[20]

8.3. General Danish Civil Penal Provisions on Jurisdiction

General rules on Danish right of punishment (jurisdiction competence) is set out in the Civil Penal Code §§ 6-12, which Code positively describes the extent of Danish jurisdiction as for criminal matters.

As for civil matters, including piracy under the Copyright Code, Denmark claims jurisdiction pursuant to §246[21] of the Civil Procedure Code, which allows Danish courts to exercise an very extensive exterritorial jurisdiction competence over subject matter codes that penalize with fines or imprisonment, for example copyright issues. However, courts have only used it in a narrow tailored fashion as the wording exceeds the scope allowed by public international law.[22] The statute covers foreign defendants that are not covered by the 1968 Brussels Convention,[23] E.U. Regulation 44/2001,[24] or a Nordic

[19] Henrik Spang-Hanssen, *Cybercrime and Jurisdiction in Denmark, Chapter 8 section 8.3.3. in* CYBERCRIME AND JURISDICTION - A GLOBAL SURVEY 170-172 (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218).

[20] Law no. 279 of 5 April 2006 [amendment to the Danish Civil Code]] (Bill no. L67/2005-06), which implement E.U. Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights, O.J. L157, 30/4/2004 pp. 45-86.

[21] See unofficial translation in Appendix 7.

[22] HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION 243-257 and 343-372 (DJØF Publishing, Copenhagen, February 2004 - ISBN 87-574-0890-1).

[23] Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters of 27 September 1968, O.J. L 299, 31/12/1972 p. 0032-0042 with adjustment in the "San Sebastian Convention," O.J. L 285, 03/10/1989 p. 0001 – 0098. A Consolidated version is published in OJ C 27, 26/1/1998 p. 0001-0027.

[24] E.U. Regulation 44/2001 of 22/12 2000 on jurisdiction and the recognition and enforcements in civil and commercial matters, O.J L 012, 16/01/2001 pp. 0001 – 0023. See on Special Parallel Treaty between E.U. and Denmark, Council Decision 2005/790/EC of 20 September 2005 on the signing, on behalf of the Community, O.J. L 299, 16/11/2005 p. 0061-069, and the Agreement between the European Community and

country. This statute gives Denmark an extremely broad jurisdiction.

Pursuant to the basic rule in §6 of the Civil Penal Code the Danish criminal jurisdiction covers acts carried out (1) in the Kingdom of Denmark (the principle of territorial jurisdiction), (2) on a Danish vessel that is outside any States public international recognized territory (3) on a Danish vessel, which is in a foreign public international recognized territory, by persons that belongs to the vessel or are traveling on it.

Furthermore, pursuant to §7 (the personal principle) subsection 1 belongs under Danish criminal jurisdiction acts that a person, which has Danish citizenship or is domiciled in the Kingdom of Denmark, has done outside Denmark, (1) as far as an act had been done outside public international recognized territory of any State, if the crime pursuant to Danish law offers a maximum penalty of more than 4 month of imprisonment, or (2)(double liability to punishment) as far as an act is done inside such a territory if it is punishable also pursuant to the legislation at that territory. Subsection 2, states that subsection one also covers acts done by a person having citizenship in Finland, Iceland, Norway or Sweden and staying in Denmark.

In addition, pursuant to §8 covers Danish criminal jurisdiction acts done outside the territory of Denmark without consideration of what State(s) the perpetrator is related to (α) when the act violates the independence, security, Constitution or public authorities of Denmark, official duties to Denmark or such Danish interests, which requires legal protection by Denmark, (β) when the act violates an obligation that the offender pursuant to law has to observe abroad, or a duty to a Danish vessel, (χ) when an act is done outside a territory of a State pursuant to international public law violates a person, which has Danish citizenship or is resided in Denmark, and the crime pursuant to Danish legislation can be punished by up to 4 month imprisonment, (δ) when the act is covered by a international instrument by which Denmark is obliged to prosecute, or (ε) when extradition of suspected persons to prosecution in a foreign State is denied, and the act, as far as it is done inside a recognized public international territory, is punishable pursuant to that territories legisla-

the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. L 299, 16/11/2005, p. 0062-0067 – reprinted in Appendix 8 of this book.

tion and the crime pursuant to Danish law can be punished with more than 1 year in prison.

§9 states, that incidents, where the punishment of an act is determined or influenced by a occurrence or premeditated result, it is regarded as if the crime was also done at the place where the consequence is taking place or is expected to take place.

If action pursuant to previous rules is taken in Denmark, the decision, as for the penalty as well as for other legal consequences, has to follow Danish law. If the incident is covered by the above mentioned §7 and the crime is done in a foreign territory recognized by public international law, then the punishment cannot exceed the maximum penalty pursuant to the legislation of the territory of the place of the crime (§10). It is a precondition as for acts done outside Denmark, that the Danish statute in question is not limited to acts done on the Danish territory, UfR 1998.1027 H.

The limit pursuant to §7, after which the sentence cannot extent the maximum penalty of the State where the criminal act was executed, also presumably apply to incidents where the basis for Danish right of punishment is §8(ε).

The Danish Justice Department is of the opinion that the above mentioned §6 and §7 subsection 1 fulfills the requirements in article 22 of the Council of Europe Convention on Cybercrime.[25]

8.4. Certain provisions on online violations

Statutes on crime can be found both in the Civil Penal Code and in special legislation, for example the Copyright Act.[26] As for the criminal sentence, a

[25] Remark no. 7.1 to bill L55 and Memorandum on the consequences of the convention from Danish Ministry of Justice to Justice-committee of the Danish Parliament, General Part – exhibit 294 – E.U. assembling 2002-03 at <http://www.folketinget/dk/Samling/20012/udvbilag/REU/Almdel_bilag294.htm> (visited 26 December 2004).

[26] On Spam, see *Rigsadvokaten* (US: Attorney General) *v. Teleselskabet* [tele-company] *Debitel*, UfR 2005.3446 H (Supreme Court of Denmark, 22. September 2005 – Docket no. 134/2005 (1. chamber)) (Held: Debitel violated § 6a, stk. 1 of the Danish Marketing Act [Markedsføringsloven] by sending 12,000 sms-messages and 36,000 unsolicited e-mails with the aim of selling different services. The Danish Consumer-

Danish court will take all crimes into consideration and issue a lump penalty, but not just sum up all the penalties into a total.

8.4.1. Hacking

8.4.1.1. Crimes related to Gaining Profit

Hacking can be used to steal, destroy or change information or software on others computers or networks.[27] These crimes are dealt with in the following statutes in the Danish Civil Penal Code.

Stealing is dealt with by §276: "Any person, who, without consent of the possessor, removes a foreign tangible movable with the intent of obtaining for himself or for others an unjustifiable gain by its misappropriation, is guilty of theft." As tangible movable in this context is also regarded energy, which is made, stored, or used to produce light, heat, power or movement or for any other economic purpose. The last sentence does not cover electronic bits-transmission and thus networks communication. The statute only covers computer-theft if this is done by use of a tangible medium, for example removal of data to a diskette that is used for transporting the information to another computer. Where the offence is of a particular crude nature or is done

Ombudsmand had claimed a penalty of 100 DKK (≈ $14) per spam-mail. The Supreme Court of Denmark cut down the penalty issued by the lower court (2 million DDK because Debitel had stopped the activity after receiving a protest-letter from the Consumer-Ombudsmand) to 400,000 DKK. The Court noted that when measuring the size of the penalty the number of addressees had to be taken into account, but it could not be based on a certain fine-size per addressee. The achieved or expected economic gain had to be taken greatly into consideration. The courts held that sms-messages had to be regarded as "electronic mail").

[27] However, hacking can also be regarded as a benefit. For example, the Danish toy company Lego cheered when it found out that enthusiast of Lego had hacked one of the company's development-tools for digital designers. The Lego leaders saw an opportunity to lean on the collective thinking of an Internet community to improve their own product while bolstering relations with committed customers, Daniel Terdiman, *Hacking's a snap in Legoland*, CNET NEWS.COM, 15 September 2005 at<http://news.com.com/Hackings+a+snap+in+Legoland/2100-1046_3-5865751.html> and Torben Daarbak, COMPUTERWORLD.DK, 16 September 2006 at <http://www.computerworld.dk/art/29810> (visited March 2006).

by a group of persons the maximum penalty is eight years of imprisonment – the normal maximum is 1½ years imprisonment.

Data-fraud: Any person, who, unlawful changes, adds or deletes information or programs related to electronic data processing or in other possible way unlawfully try to influence the result of such data processing, with the intent for himself or others to gain unjustifiable profit, are guilty of data-fraud. The statute requires that the criminal has broken into (messed with) the data-process. Where the crime is of a particular crude nature or is done by a group of persons the maximum penalty is eight years of imprisonment – the normal maximum is 1½ years imprisonment, §279a. Use of false electronic money is regarded as either fraud (§279) or data-fraud (§279a).[28] Electronic money is pursuant to §169 subsection 2 means, which without being genuine nevertheless can be use as such. §169 make it illegal to achieve or produce false electronic money.

> *Prosecutor v. T*, UfR 2000.1181 Ø (Courts of Appeals for Eastern District, 2000) – Passed sentence - as charged - for attempt of data-fraud pursuant to §279a for 22 withdraws and attempts hereto over a period of 2½ hours and in connection with possession of 123 false debit cards, all cards related to a bank in Moscow.

Theft done by electronic bits-transmission is covered by §293 that deal with the issue of taking without the owner's consent (TWOC). Where the crime is more systematic or of an organized nature or where the "borrowed" item is not returned after use the maximum penalty is two years imprisonment – otherwise the normal maximum is one year.

> *Prosecutor v. T*, UfR 1978.1003 Ø (Courts of Appeals for Eastern District, 1978) - Convicted a person pursuant to §293 for illegally connecting to a community antenna (by taking without the owner's consent) since such a hooking-up could only be motivated with the aim of getting access to the programs, that is, the information which was transmitted by the system.

Illegal acts done by bits-transmission can also be punished pursuant to other

[28] Section no. 3.1.1 of remark to bill no. L 55 of 5 November 2003, enacted as law no. 352 of 19 May 2004.

statutes.

A person that destroy, damage, or remove things belonging to others can pursuant to §291 be punished for criminal damage. An example would be to change the content of a webpage. If the damage is substantial and done with intent, a sentence of six years imprisonment can be issued. This statute covers incidents where a person willfully spreads virus-software via the Internet, Denial-of-Service (DoS), Ping of Death, and situations where data has been made inaccessible for the user.[29] It also covers incidents of deleting data or software. A panel of experts writing White Paper no. 1032/1985 were not sure whether §291 could be used where the unlawful act is distortion of data while these are being transmitted.[30] If done by gross negligence the maximum penalty is 6 month in prison.

> *Prosecutor v. T*, UfR 1987.216 Ø (Courts of Appeals for Eastern District, 1987) - Media for carrying data and containing data regarded as "things." Held that T had committed criminal damage pursuant to §291 by, not deleting a user file directory (UFD) but removing it to another master file directory (MFD) and changing the name of the UFD, which meant the file could not be printed. The court did not distinguish between the physical media and the content, but determined on basis of all the facts. It pointed out that an aggravating circumstance was the fact that to undo the criminal acts external computer expert had been needed. The principal criminal was also sentenced for having laid "logical bombs" that deleted all relevant user files. They received 6 years in prison pursuant to subsection 2.

§293 are used in situations with misuse of such telecommunication that requires a physical connection to other equipment. In case of use of a cellular phone the act is regarded as data-fraud, §279a.

If the act causes interference in the operation of common communication, public mail delivery, telegraph- or phone-installations, radio- or TV-installations, information systems or installations, which serves common supply of water, gas, electricity or heating, the maximum penalty pursuant to

[29] *Id.* remark no. 13.

[30] The panel held § 263 (closed content) could be used. White Paper 1417 of 2002 from the Justice department's Expert panel on economic and data crimes <http://www.jm.dk/wimpdoc.asp?page=document&objno=64938> (visited 15 December 2004).

§193 six years of imprisonment. In case of gross negligence, the maximum is 6 months in jail. This statute includes computer systems/installations that are of importance for public use, for example attacks against central functions on computer networks, host servers, and banks computer systems.[31]

> *Rigsadvokaten* (US: Attorney General) *v. Teleselskabet* [tele-company] *Debitel*, UfR 2005.3446 H (Supreme Court of Denmark, 22 September 2005) (T send 12,000 SMS-messages and 36,000 e-mails to certain receivers with purpose of selling services. Held: Marketing Act been violated. Penalty of 2 million DKK (~ $308,000) for causing the receivers a nuisance, the improper formulation in the e-mails, and the gained profit. SMS-messages not regarded as "electronic mail").

8.4.1.2. Crimes related to Peace, Privacy and Honor

Pursuant to §263 subsection 2 a person, that unlawful achieves access to others information or programs, which is intended for use in a information system, will be punished with up to 1½ years imprisonment The statute includes incidents where a person unlawfully opens an electronic message. If the intent is to get access to information of a firm's business secrets, or in other important circumstances, or where criminal acts are of a more "systematic or organized nature" the maximum penalty is six years in prison (subsection 3).[32] The statute cannot be used where the criminal has misused his rightfully achieved access to the (confidential) information, or for example opening an e-mail which content wrongfully as been sent to the person opening the e-mail.

[31] *Id*.

[32] *U.S. v Scott Levine* (United States District Court, E.D. Arkansas. (Little Rock) Feb 2006) (Eight years in prison for breaking into Acxiom's servers and downloading gigabytes of data from the world's larges repository of consumer data related to major banks, credit card companies and the U.S. government. Levine downloaded an encrypted password file and then ran a cracking utility. There was no evidence the data had been used for identity fraud), Declan McCullah, *Data thief gets eight years*, NEWS.COM 24 February 2006 at <http://news.com.com/2100-7348_3-6042290.html> and <http://www.newsinferno.com/archives/883> (visited March 2006).

> *Prosecutor v. T*, UfR 1996.979 Ø (Courts of Appeals for Eastern District, 1996) – A bank clerk was acquitted for charges under §263 subsection 2 for having accessed the bank's computer system and thereby achieved certain business secrets. He had used his own password but accessed information not related to his job-position, from which he had been dismissed.
>
> *Prosecutor v. T*, UfR 2000.1450 Ø (Courts of Appeals for Eastern District, 2000) – Sentence pursuant to §263 subsection 2 for having attempted to install a program, which failed because of an installed anti-Back Office program, and for having taken possession of another person's user-ID and password. Computer confiscated.

Whether the crime is "systematic or organized nature" will depend on the situation and the facts. The term is related to article 7 Proposal for a Council Framework Decision on attacks against information systems[33] which aims to make it a crime to participate in a criminal organization in the E.U. Member states, except that the maximum sentence is not used. However, the term in the Danish statute is not limited to activities done by a criminal organization as defined in the E.U. Framework. Other forms of systematic or organized hacking can be regarded a more severe circumstance that will allow use of subsection three.[34]

A person, that unlawfully commercially sells or to a broader number of persons informs of a code or other access means to a non-commercial information system and whereto access is protected by a code or other special access-feature, can be sentenced up to 1½ years of imprisonment. In severe circumstances, for example where the passing on has "a large amount" or causes severe risk for large damage the maximum penalty is six years in prison, §263a. The statute includes private PCs and systems that are intended for single-users or a small user group, businesses internal information systems and central systems. The term "a large amount" is presumed to be at least ten codes. In circumstances, where the dissemination has been done several times but by less than 10 codes, use of subsection two will require that there is such a close connection in time that the successive acts can be regarded as one total.

[33] COM/2002/0173 final – CNS 2002/0086 */,* O.J. C 203 E, 27/08/2002 p. 0109 – 0113.
[34] Remark no. 9 to bill L 55 of 5 November 2003, enacted as law no. 352 of 19 May 2004.

Use of §263a is precluded in instances of possession or acquisition of codes or other access means or where non-commercial dissemination of one or a few codes. Such acts might be penalized as an attempt or accessory to hacking, confer §263, stk. 2 with §21 or §23.[35]

Where a person unlawfully achieves or spreads a code or other access means to a commercial information system, whereto access is reserved for paying subscribers, the normal maximum penalty is 1½ years imprisonment, §301a. In "severe circumstances" the maximum penalty is the same as for §263a. The pure possession of such access means is not covered by the §301a.[36] The statute includes all access means to commercial information systems, for example decoder cards, calling cards (phone pin codes), NUI codes etc. Getting or dissemination of one single code or access means is enough to trigger the statute. As "severe circumstances" are regarded incidents where dissemination is done via the Internet to a larger closed group of people, for example a club on the Internet having a larger number of members.[37]

Pursuant to §264c a person is under the same penalty as in §263 if he, without having been an accessory to the main crime-acts, achieves or unlawfully uses information that has been gained by a crime mentioned in §263, for example hacking.

> *Prosecutor v. T*, UfR 1996.1538 Ø (Courts of Appeals for Eastern District, 1996) – A law firm had sent a hard disk to destruction at a burning-centre plant without effectually having deleted personal information on the hard disk. The information came in the possession of a journalist, which wrote about data security and used the information as an example. A court decision

[35] Remark § 1 no 10 to bill L55 of 5 November 2003, enacted as law no. 352 of 19 May 2004. Denmark in time has implemented the E.U. Copyright Directive of 2001, opposite Italy, Luxembourg, Belgium, Finland and Sweden. The Norwegian government has proposed a new copyright law to make it illegal for Norwegians to copy songs from their own CDs onto MP-3 players, but legal to do so for making a CD duplicate. The new proposal would allow fines and a maximum penalty of three years in prison for violating copyrights and engaging in computer piracy.

[36] White Paper 1417 of 2002, see *supra* note 27.

[37] Remark § 1 no 16 to bill L55 of 5 November 2003, enacted as law no. 352 of 19 May 2004.

> using §264c ordered the hard disk and diskettes, whereto the information had been copied, handed over to the law firm.

§264d criminalize a person that unlawful distributes messages or pictures that relates to another persons private sphere or pictures of a person taken under circumstances that can obviously be required to be kept form the public. The provision includes messages or pictures relating to deceased persons and has a maximum penalty of 6 months imprisonment.

> *Prosecutor v. T*, UfR 1999.177 V (Court of Appeals for Western District, 1999) - A scorned husband T published on his website seven nude pictures of his ex-wife, each with an offending text, together with her social security number, address, and phone number. For this spiteful spreading of information on the Internet, T was sentenced to 20 days of mitigated imprisonment pursuant to §264d and §232.[38]

8.4.2. Piracy

The Danish Copyright Act[39] §76 subsection 1 penalizes a person, that with intent or gross negligence violates the Act's statutes on copyright protection, or the rights belonging to creative artist, creators of sound recording, motion

[38] In what seems to be a similar case in Canada, a man who used the Internet to turn his ex-girlfriend's life upside down was convicted for criminal harassment and sentenced to one year in jail, see *Cyberstalker sentenced to one year*, CBC News, 16 March 2006 <http://www.cbc.ca/story/canada/national/2006/03/16/cyberstalk060316.html> (visited 18 March 2006). A Dutch Appeal Court ruled in June 2006 in Brein v. Techno Design that a Dutch music website, which links to mp3 files had to stop promoting the infringement of artist right and copyright. The court held that a warning to users on zoekmp3.nl not to infringe copyright did not excuse Techno Design from liability, at "such a warning ignores the reality that the lion's share of visitors are looking for unauthorised mpP3 files," REUTERS, *Dutch site linking to MP3 files loses court case*, 19 June 2006 at <http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2006-06-19T105335Z_01_L19632414_RTRUKOC_0_US-INTERNET-MUSIC.xml> (visited July 2006).

[39] The latest consolidated version of "lov om ophavsret" is printed as no. 725 of 21. December 2005 30 June 2004 with amendment from laws no. 1402 of 21/12/2005 and 1430 of 21/12/2005.

pictures, radio and TV-broadcasting, photo pictures, makers of catalogues etc., with a fine.[40] If the reproducing crime is done with intent and in "severe circumstances", the maximum penalty in the Act can rise to 1½ years, unless the crime is covered by §299b in the Civil Penal Code (see below).[41]

"Severe circumstances" are especially present if the crime is part of a business, if a significant number of copies are produced or spread to the public, or if creations or productions are reproduced in such a manner that the public gets access to the reproductions at a individual chosen place and time, §76 subsection 2. The violation of the exclusivity of copyright to availability is in itself a severe circumstance. Availability of creations etc., for example via uploading to a homepage or other distribution via open computer networks such as the Internet, so that the public gets access, is covered by subsection 2, even if the disperse is non-commercial.[42]

If the reproduction is done outside Denmark under such circumstances that in Denmark it would be violating the Act, then a person, that imports such reproductions with intent to give the public access to them, pursuant to §77 can be penalized with a fine.[43] In severe circumstances the penalty is as mentioned for §76 subsection 2.

Civil Penal Code §299b: A person, that for profit for himself or others, unjustifiable gains or under special gross circumstances makes severe copyright infringements, confer §76 subsection 2 in the Copyright Act, or participates in illegal import of severe nature, confer §77 subsection 2 of the Copyright Act, can be sentenced up to six years in prison. The statute requires the crime

[40] A survey on teenagers in Denmark show 85.9 percent thought is was all right to copy music or movies, and that 79.5 percent had done it, 58.5 percent think it is ok to take the bus or train without paying, while only 4.8 percent think it is all right to steal, page 20 of Rigtigt og forkert [Right or Wrong] from Børnerådet [Danish Children's Council] (Copenhagen 2006 – ISBN 87-90946-36-7) at <http://www.boerneraadet.dk/graphics/pdf-filer/andet/Rigtigt%20og%20forkert.pdf> (visited April 2006).

[41] By Law no. 279 of 5 April 2006 om ændring af retsplejeloven was added chapter 29a & §653 subsection 1 to the Civil Procedure Code about court's ability to order giving information related to violations of intellectual property, and made changes on rules of evidence. Confer footnote 16 above

[42] Remark 2.3.3.1 and § 4 no. 1 to bill L55 of 5 November 2003.

[43] Section 2.3.3.1 of remark to bill L55 of 5 November 2003.

or import is of a severe gross nature, which is especially the case if the act is done with purpose to give the perpetrator or others an unlawful profit. Other severe gross copyright violations can also imply use of §299b, for example because the violations has such a proportion that the copyright owner has had extreme losses, or risk hereof. §299b is presumed to be used where the violation is deemed to be so gross that the reaction of the public should be pursuant to the Civil Penal Code rather than the Copyright Act, or where the violation relates to individual very expensive software or systems, which for example has been developed for one or more businesses.[44]

Blocking devices are dealt with in §78 of the Copyright Act, which penalize with a fine a person that with intent or gross negligence: "(A) sells or commercially posses means which sole purpose is to make it easier to remove or circumvent technical devices that protects software; (B) without permission to circumvent efficient technical devices, or to produce, import, spread, sell, lease, advertise for sale or rent of or for commercial purposes possess devices, products or components which circumvent technical devices – including service, but excluding software and does not hinder research on encryption; (D) without permission to remove or change electronic information about administration of rights or make distribution of copies, import with purpose to make distribution or transfer to the public of creations or other products where the electronic information of the rights of the owner have been removed or changed without permission and the person knew or should that know that the act was a violation of the Copyright Act."

> *Prosecutor v. T* (Court of Appeals for Western District, 20. April 2001 – Dockets No.: V.L. B-1943-99 & V.L. B-2089-99) - Held: T through his website was forbidden to make deep links to illegal published music accessible on the Internet; and forbidden to copy or help others to illegal coping music on the Internet. 100.000 DKK (~ $ 15,400).
>
> *Danske Dagblades Forening v. Newsbooster*, UfR 2003.1063 SH (The Maritime and Commercial Court in Copenhagen 19 February 20003) - Internet Service use of newspaper's headlines and using deep links directly to articles

[44] Section 2.2.3 and § 1 no. 14 of remarks to bill L55 of 5 November 2003, enacted as law no. 352 of 19 May 2004.

in newspaper - without going through the newspapers homepage - was a violation of the Copyright Act § 71.

Home A/S v. OFIR A-S (previous: Søndagsavisen a-s) (The Maritime and Commercial Court in Copenhagen, 24 February 2006 - docket No. V-108-99), <http://www.domstol.dk/media/-300011/files/v010899.pdf> - OFIR on the Internet made a housing service by copying data – deep linking - from the database produced by and related to the plaintiff homepage. Additional defendant used deep links to plaintiff's website going around plaintiff's homepage. Defendant was acquitted on all accounts/claims.
The court pointed out that the main goal with the protection of databases in the E.U. Database Directive[45] is to stimulate the creation of search, storage and processing systems for existing information with the aim of exchange of information, but for the process of producing material that later can be gathered in a database.
Furthermore, the court remarked that search-services, which will become steady more common on the Internet, are desirable as a necessary function of today's Internet as media for search and exchange of a huge and steady expanding amount of information. The database-protection, which is the aim of the E.U. Database Directive,[46] reflects such wishes. It must be regarded as ordinary that search services uses deep linking, whereby the customer in an effective way comes directly to the desired information. In the way the Internet is constructed and is functioning, this must be in compliance with the interest of those who chooses to use the Internet to make accessible information for the public. Therefore, the actors, including providers, on the Internet must expect deep linking.

Telecompany TDC v. IFPI Danmark (on behalf of Danish Musicians and Artist Associations) (Supreme Court of Denmark, 10 February 2006 – Docket 49/2005) – Through two Internet-servers a large number of music was made available without consent of the owner of the music. The owners of the serves were subscribers at TDC. The Supreme Court affirmed a lower court's decision of issuing an injunction ordering TDC to stop transmission. An injunction was reasonable considering the copyright owners interests and the trouble of TDC fulfilling the order. The Court rejected TDC's arguments that it was free of liability and punishment pursuant to the Danish E-Commerce Act (confer the E.U. E-Commerce Directive) and even though it had no knowledge of the content of the information going through its servers.

[45] Directive 96/9/EC of 11 March 1996, O.J. L 77, 27/03/1996 pp. 0020-0028.
[46] Directive 2000/31/EC of 8 June 2000, O.J. L 178, 17/07/2000 pp. 0001-0016.

As Norwegian legislation to a very large extent copies E.U. legislation with a Nordic "stamp" should at this place be mentioned a case involving a Norwegian teenager, Jon Lech Johansen, that had been sued both in Norway and in the U.S. in connection with his participation in developing circumvention software so it was possible to show DVDs in the Linux operating system. The civil case in U.S. is *DVD Copy Control Association v. Andrew Brunner, Jon Lech Johansen, Masters of Reversed Engineering (MoRE)*, et. al., 10 Cal.Rptr.3d 185, 116 Cal.App.4th 241 (Cal.Ct.App.6.Dist., February 27, 2004). The criminal Norwegian case can in an unofficial translation into English be found as *Procecution v. Jon Lech Johansen* (Oslo First Instance court (criminal division), 7. January 2003 - Docket 02-507 M/94) at <www.geocities.com/hssph/DVDjon2.pdf> and *Procecution v. Jon Lech Johansen*, LB-2003-00731 (Borgating Appellate Court, 22 December 2003 - Docket 03-00731 M/02) at <www.geocities.com/hssph/DVDjon1.pdf>. Johansen was acquitted for all charges in Norway in both the trial and the appeal court.

8.4.3. Forgery

Forgery is penalized in §171 with up to 2 years imprisonment. In severe circumstances or a larger amount of forgeries 6 years. Subsection 2 defines a document as a written or electronic statement bearing the name of the author that appears to being decided to serve as evidence. The statute does not require any specific security means as for the electronic expression, as for example a requirement of an electronic signature.[47] Neither does the statute require that the issuer's manifestation have the characteristic of a signature. The statute does only cover documents that have the purpose of issuing legal intent, thus serving as evidence. However, the statute does not cover documents dealing with rights.

8.4.4. Means of Payment

§301 penalize up to 1½ years imprisonment of a person, that with intent of illegal use produce, achieves, posses or disseminates (a) information that

[47] Section 4.3.1. of remark to bill L55 of 5 November 2003, enacted as law no. 352 of 19 May 2004.

identifies means of payment issued to others, or (b) generate debit card numbers. The statute does not include real credit cards. It includes all debit cards, no matter how the necessary information on payment has been achieved. If the dessimation is done to a larger group of people or in other severe circumstances, the maximum sentence can be 6 years prison, for example to an Internet group consisting of a larger group of people.

8.4.5. Crime relating to Sexual Morality

A general statute against immoral pictures and pornography was abolished in 1969, see above section 8.2.1.

A person, that through indecency outrages public decency or gives public nuisance, can be sentenced up to four years in prison, §232.

> *Prosecutor v. T* , UfR 1999.177 Ø (Courts of Appeals for Eastern District, 1999) – A disdained husband T published on his website 7 naked pictures of his ex-wife, each with an offending text, together with her social security number, address and phone number. For this spiteful spreading of information on the Internet, T was pursuant to §264d and §232 sentenced to 20 days mitigated imprisonment.

Furthermore, the court can issue a restraining order prohibiting the criminal from staying in public parks, schools, playgrounds, reformatory, mental hospital and institutions for handicapped persons, in specific mentioned woods, swimming pools and beaches, §236. Disobeying the order can be penalized by up to 4 month in prison.

> *Prosecutor v. T*, UfR 2001.2573 Ø (Courts of Appeals for Eastern District, 5. September 2001) – 24 year old T was charged for violation of §264 d and §232 because he on a Internet website under the profile "Lovers" had put a text pursuant to which a 15 old female, given pet name and an address, wanted different kinds of sex with experienced men. This had the effect that a 13-year-old girl, whose name and address was very much similar to the information on the website, received sexual enquiries from several men. T's acts, on the Internet by making the text with sexual orientation and wishes, was a violation of §264 d, even though the information of the girl was untrue. By uploading the text T could expect the 13 year girl would be contacted by men with offers that for a young girl was an unusual sexual behavior, including anal sex, thus T was regarded as been accessor to violate her decency pursuant to §232 and §23. T was sentenced to 20 day in prison and pay 3.000 EURO in damages.

If a person sells indecent pictures to a person under sixteen of age, the criminal can be fined, but not imprisoned, pursuant to §234.

Child pornography is dealt with in §235, which statute was amended last in 2003[48] amongst other with the purpose of making the necessary amendments for Denmark to be able to participate in a E.U. Framework on combating the sexual exploitation of children and child pornography to which the Commission had put forward a proposal in January 2001[49] Furthermore the amendment has taken into consideration the protocol of 25 May 2000 from U.N. General Assembly on the sale of children, child prostitution and child pornography,[50] which protocol Denmark signed on 7 September 2000.

Subsection 1 of §235 states: A person, which distributes obscene pictures, or film, other obscene visual presentations "or similar" of persons under the age of eighteen, is penalized with a fine or imprisonment up to two years or in "severe circumstances" with up to six years in prison "Severe circumstances" is especially instances where the child's life is put in danger, where gross violence is used, where the child is serious injured, or where the spread is of more systematic or organized nature. Subsection 2: A person, who possess or through consideration makes himself familiar with obscene pictures or films, obscene visual presentations "or similar" of persons under the age of eighteen, can be penalized with a fine or imprisonment of up to one year. Subsection 2 does not cover possession of obscene pictures of a person over the age of fifteen, if that child has permitted the possession. "Or similar" covers commercial presentation or lease of child pornography.[51]

§235 only deals with real pictures or films, whereas cartoons, computerized produced pictures and other productions that illustrates sexual attacks of a child and which has not happen in reality, is not made a crime.[52] "Obscene" is a legal standard that varies with time and place. Pictures of children in situations of sexual intercourse or other sexual excesses are regarded as "obscene." The main emphasis is set at whether the picture shows a child, that

[48] Law no. 228 of 2 April 2003 based on White Paper 1377/1999 on child pornography and cyber crime investigation.

[49] O.J. C 062 E, 27/02/2001 p. 0327-0330. This has become Council Framework Decision 2004/68/JHA of 22 December 2003, O.J. L 13, 20/01/2003 p. 004-0048.

[50] A/RES/54/263.

[51] Section 2.1.4 of Remarks to Bill no. L117, enacted as law no. 228 of 30 September 2003.

[52] *Id*.

participate in sexual activities, or a child against which it can presumed that the picture taking has required some gross offensive acts, for example by using the child as model for photographing genitals, or of sexual touch or contacts.

If a picture or similar has an artistic value this might legitimize it and thus not be covered by §235.[53]

Pursuant to the commentary to the bill that amended §235, a person is not regarded as having possession of a picture that momentarily is moved from a database to the persons own computer. However, if the person on a hard disk or diskette stores the picture so the person for long-term purpose can recall the picture again, then the picture is regarded as being in the possession of the person.[54] More fortuitous situations, where the Internet user accesses network areas or websites whereto there is free access to child pornography, is not covered by §235.[55]

> Denmark has made the following reservations to Article 9 of the Cybercrime Convention related to Child Pornography:
>
> The criminal area according to Article 9 shall not comprehend the possession of obscene pictures of a person attained the age of fifteen, if the person concerned has given his or her consent to the possession, cf. Article 9, paragraph 1, letter e.
>
> The criminal area according to Article 9 shall not comprehend visual representations of a person appearing to be a minor engaged in sexually explicit conduct, cf. Article 9, paragraph 2, letter b.

[53] See page 40-41 in White Paper 435/1966 on penalty of pornography and Folketings Tidende [Official Journal of Danish Parliament - hereinafter F.T.] 1999-2000, Supplement A, column 7800.

[54] F.T. *supra* note 46, 1994-95, Supplement A, column 473. See also White Paper 1377/1999, page 57.

[55] Section 2.1.5 of Remarks to Bill no. L117, enacted as law no. 228 of 30 September 2003.

CHAPTER 9

Jurisdiction Rules of Denmark & "pure online" dealings outside the European Union on international computer networks

By Henrik Spang-Hanssen[1]

This chapter deals with the question of personal jurisdiction in cases of trans-border dealings on international computer networks.[2]

The rules on personal jurisdiction belongs to the group of procedural rules, which lay down the conditions to allow a court to deal with a (international) case - opposite material rules that relates to the rights and duties the legal system gives or prescribe each legal person.[3] When determining the international competence of Danish courts Denmark is regarded as one jurisdiction, and one speaks of the courts international competence or jurisdiction-rules.[4]

[1] This chapter is in an older version available in a Danish translation at <www.geocities.com/hssph>.

[2] See some abbreviations in Appendix 10.

[3] Some scholars divide international jurisdiction into "legislative" and "enforcement", while others, particularly in U.S., further splits the first into "prescribe" and "adjudicative" jurisdiction, HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION chapter 25, including note 789 (DJØF Publishing, Copenhagen, February 2004 - ISBN 87-574-0890-1) [hereinafter SPANG-HANSSEN-2].

[4] An introduction in English to the Danish civil procedure is made by ERIK WERLAUFF, CIVIL PROCEDURE - DENMARK (1 Ed. 2001, DJØF Publishing - ISBN 87-574-0496-8).

Thus, the question at issue is whether courts in Denmark at all have competence in a specific case.[5]

The article does not deal with issues that involves tangible effects, as use of international computer network in relation to tangible effects should only be regarded as issues belonging to the category of old times mail-orders.[6] The new issue caused by the emerge of international computer networks is that certain effects, which previous had to be "transported" in the form of tangible effects, now can be "transmitted" by electronic bits (and that the transport route is fortuitous and unpredictable).[7] Further, the article will not include pure "correspondence" communications by international computer network. The main issue of the article is "*pure online*" commerce/service.

Considering the conditions of actions that only exist of bits-transmission, such as online deliverance of software combined with online payment hereof, the one party is often located outside the area of the European Union.[8] An

[5] ALLAN PHILIP, DANSK INTERNATIONAL PRIVAT- OG PROCESRET 81 [Danish International Private- and Procedural law] (3 ed. DJØF Publishing, Copenhagen 1976 - ISBN 87-574-1962-0) [hereinafter ALLAN PHILIP].

[6] Danish law does not know the common law distinction between jurisdiction in personam and jurisdiction in rem, Allan Philip, *American-Danish Private International Law* 24 in BILATERAL STUDIES IN PRIVATE INTERNATIONAL LAW no. 7 (Ed. Arthur Nussbaum, Oceana Publications, New York 1957).

[7] It is increasingly clear that modern businesses no longer require an actual physical presence in a state in order to engage in commercial activity there, *Gator.com Corp. v. L.L. Bean, Inc.*, 341 F.3d 1072, 1081 (US Federal Courts of Appeals for 9th Cir. September 2003)

[8] On E.U. jurisdiction-rules and e-commerce, see JOAKIM S.T. ØREN, INTERNATIONAL JURISDICTION AND CONSUMER CONTRACTS – SECTION 4 OF THE BRUSSELS JURISDICTION REGULATION ((Complex 5/04, Norwegian Research Center for Computers and Law, Oslo University 2004, ISBN 82-7226-082-4), JAN TRZASKOWSKI, LEGAL RISK MANAGEMENT IN ELECTRONIC COMMERCE – MANAGING THE RISK OF CROSS-BORDER LAW ENFORCEMENT (Ex Tuto Publishing, 2005 – ISBN 87-991018-0-7), KIM ØSTERGAARD, ELEKTRONISK HANDEL OG INTERNATIONAL PROCES- OG PRIVATRET (DJØF Publishing, Copenhagen 2003 - ISBN 87-874-0969-2). The Japanese Government has in February 2006 proposed a rule on jurisdiction for consumer protection similar to the one in the European Union, that is, in consumer contracts the consumer can sue the vendor at the court in the plaintiff's forum and the local consumer protection-rules are overriding a online contract, see *Japanese government Pushes Choice of Law Protection for Citizens Making Online Deals*, BNA's Electronic Commerce & Law, 22 February 2006,

overwhelming part of software is developed in the U.S. and Asia with sales done through websites managed and located from outside the area of the European Union. Therefore, the jurisdiction-rules in the Brussels Convention[9] and the E.U. Regulation 44/2001,[10] are not feasible,[11] whereas each of the E.U. Member states' national jurisdiction-rules has to be used. Thus, as

Vol. 11 No. 8 page 214, at <http://pubs.bna.com/ip/bna/eip.nsf/eh/a0b2h3g4g3> (visited March 4 2006).

[9] Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters of 27 September 1968, O.J. L 299, 31/12/1972 p. 0032-0042 with adjustment in the "San Sebastian Convention," O.J. L 285, 03/10/1989 p. 0001 – 0098. A Consolidated aversion is published in O.J. C 27, 26/1/1998 p. 0001-0027.

[10] Denmark and the E.U. has made a so-called parallel treaty that makes the rules of the E.U. Regulation 44/2001 of 22/12 2000 on jurisdiction and the recognition and enforcements in civil and commercial matters, O.J. L 012 , 16/01/2001 P. 0001 – 0023, to be used between Denmark and the other E.U. Member States, see Council Decision 2005/790/EC of 20 September 2005 on the signing, on behalf of the Community, O.J. L 299, 16/11/2005 p. 0061-069, and the Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. L 299, 16/11/2005, p. 0062-0067 – reprinted in Appendix 8 of this book. The vital reports related to the Brussels Convention, the Lugano Convention and the E.U. Regulation 44/2001 of 22/12 2000 on jurisdiction and the recognition and enforcements in civil and commercial matters are: Jenard Report no. 1 (1979), O.J. C59, 5/3/1979, p. 0001-0065 at <http://aei.pitt.edu/1465/01/commercial_report_jenard_C59_79.pdf>, Jenard Report no. 2 (1979), O.J. C59, 5/3/1979, p. 0066-70 at <http://aei.pitt.edu/1466/01/commercial_reports_jenard_protocols_c59_79.pdf>, the Schlosser Report (1978), O.J. C59, 5/3/1979, p. 0071-0151 at <http://aei.pitt.edu/1467/01/commercial_reports_schlosser_C_59_79.pdf>, and the Jenard-Möller Report (1990), O.J. C 198, 28/7/1990, p. 0057-00122 at <http://aei.pitt.edu/1464/01/Commercial_reports_Jenard_OJ_C_189_90.pdf> (visited March 2006).

[11] These covers as of May 1st 2004 only 24 States out of circa 200 States in the World that is connected to international computer networks. The Internet users of E.U.'s only amount to 2.6 % of the total World population, see Table 15 and Appendix A in SPANG-HANSSEN-2 *supra* note 3. One third of the users of the Internet lives in Asia and the numbers are growing rapidly. China has since 1996 by drastic amendments of the law in a large degree copied statutes from U.S., which thereby have even greater use than the laws of E.U. Thus, the latter has a decreasing effective on the international computer network.

for Denmark in a large degree of cases of "pure online" dealings the rules of the Danish Civil Procedure Code [hereinafter Rpl.] shall be used.[12]

Initially should be pointed out that the Danish jurisdiction-rules does not allow courts in Denmark to reject cases, even though the judge feels it is unfair to adjudicate a certain case causes by the international aspects of the case - here, transborder transmission of electronic bits on international computer networks.[13] In Denmark a court does not have any discretion to reject a case as long as it is in accordance with the rules of international jurisdiction. The doctrine of forum non-convenience[14] is not used in Denmark.[15]

Thus, the courts in Denmark have competence in all cases with international aspects. However, the question arises, whether the Danish court system

[12] 77 percent of the Nordic users surfs directly on the American Yahoo's ".com" rather than on the Nordic languaged websites on yahoo.dk, yahoo.sv and yahoo.no, Magnus Bredsdorff & Jakob M. Larsen, *Yahoo lukker i Danmark - tabte 66 millioner* [Yahoo shut down in Denmark - 66 millions in loss], COMPUTERWORLD-DK, 22 January 2004 at <http//: www.computerworld.dk-default.asp?Mode=2&ArticleID?22289> (visited 24 January 2004).

[13] Such a discretionary possibility should be amended, Joseph M Lookofsky, *Godsværneting og 'Due Process of Law'* [The "Goods-jurisdiction-rule" and 'Due Process of Law'], JOURNAL OF LAW PART B 1985B.73, 77-78 and HENRIK SPANG-HANSSEN, CYBERSPACE JURISDICTION IN THE U.S.: THE INTERNATIONAL DIMENSION OF DUE PROCESS 387 (Complex 5/01, Norwegian Research Center for Computers and Law, Oslo University 2001 - ISBN 82-7226-046-8 – US Congress Library 2003450386), free download from <www.geocities.com/hssph> [hereinafter SPANG-HANSSEN-1].

[14] The court cannot reject to deal with a case even though is has inferior or insignificant or no contact to the courts own legal system.

[15] GOMARD, CIVILPROCESSEN [Civil Procedure] 129-130 (5. Ed. v/Kistrup, GadJura Publishing, Copenhagen 2000 - ISBN 87-619-0204-7) [hereinafter CIVILPROCESSEN], ALLAN PHILIP *supra* note 5, at 94 , PETER ARNT NIELSEN, INTERNATIONAL PRIVAT- OG PROCESRET [International private- and procedure law]104 (DJØF Publishing, Copenhagen 1997 -87-574-7630-6) [hereinafter ARNT NIELSEN]. The doctrine is neither used in Norway, HANS PETTER LUNDGAARD, GAARDERS INNFØRING I INTERNASJONAL PRIVATRETT [Gaarders introduction to international private law] 33 (3 Ed., Universitetsforlaget AS, Oslo, 2000 - ISBN 82-00-45239-5). Opposite, the doctrine is used in Sweden, MICHAEL BOGDAN, SVENSK INTERNATIONELL PRIVAT- OG PROCESSRÄTT [Swedish international private- and procedure law] 113 (5. Ed., Norstedts Juridik AB, Stockholm 1999 - 91-38-50115-5).

has capacity to deal with all the cases involving websites on the international computer networks that daily (in 1991 figures) is added by somewhat 1,5 million new webpages, which can be accessed by every person connected to the international computer networks. As mentioned below, the Danish jurisdiction-rules do not require the case has any special connection to Denmark as several of the jurisdiction-rules is based on other factors. Public international law - not each State's private international law - orders (beyond the requirement of a close link) predictability and fundamental fairness. This cannot be said to be obtained by all the rules of the Danish Civil Procedure Code when the issue is transborder dealings on international computer networks outside the area of the European Union.[16]

The starting point in any case involving the Internet should be that the case is international rather than national.[17] The new issue is that for example any website reach every jurisdiction (unless special access-features is incorporated on the homepage) thus new requirements or factors has to be implemented in previous rules on jurisdiction.

Pursuant to international procedural rules Danish courts lacks competence if a sufficient links to Denmark does not exist. The points of contact in public

[16] Use of the exorbitant jurisdiction rule in the Danish Civil Procedure Code [hereinafter Rpl.] § 246 is prohibited for the areas covering the E.U. and Lugano conventions on jurisdiction, see Danish Act no. 325 of 4 June 1986 on the Brussels Convention, Article 3 preamble no. 2 of the Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters of 27 September 1968, O.J. L 299, 31/12/1972 p. 0032-0042 with adjustment in the "San Sebastian Convention," O.J. L 285, 03/10/1989 p. 0001 – 0098 (A Consolidated version is published in O.J. C 27, 26/1/1998 p. 0001-0027), and Article 3 of the E.U. Council Regulation 44/2001 of 22. December 2000 on jurisdiction and the recognition and enforcements in civil and commercial matters, O.J. L 012, 16/01/2001 pp. 0001 – 0023, and Article 3 of the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters of 16 September 1988, O.J. L 319, 25/11/1988, p. 009-0048. Can also be found at <http://www.curia.eu.int> or <http://europa.eu.int/cj/common/recdoc/convention/en/index.htm> (visited January 2004).

[17] The Internet is not restricted by distance or territorial boundaries, *Reno v. American Civil Liberties Union*, 521 U.S. 844, 851 (US Supreme Court 1997)(noting that "cyberspace" is accessible to anyone, located anywhere, with Internet connection).

international law[18] is not necessarily the same as in (Danish) private international law;[19] and the requirements in public international law is different for legislative (prescribe and adjudicate) and enforcement jurisdiction.[20]

Professor F.A. Mann has summarized jurisdiction in international law as follows:

"A State has legislative jurisdiction if its contact with a given set of facts is so close, so substantial, so direct, so weighty that legislation in respect of them is in harmony with international law and its various aspects (including the practice of States, the principles of non-interference and reciprocity and the demands of interdependence). A merely political, economic, commercial or social interest does not in itself constitute a sufficient connection."[21]

Professor Ian Brownlie has summarized that international law "is developing in the light of the following principles:[22]

- the territorial theory, while remaining as foundation of the law, fails to provide ready-made solutions for some modern jurisdictional conflicts
- a principle of substantial and genuine connection between the subject matter of jurisdiction, and the territorial base and reasonable interests of the jurisdiction sought to be exercised, has to be observed.
- extra-territorial acts can only lawfully be the object of jurisdiction if:

[18] SPANG-HANSSEN-2 *supra* note 3, Chapters 27 and 32.

[19] ALLAN PHILIP *supra* note 5, at 85-86.

[20] F.A. Mann, THE DOCTRINE OF JURISDICTION IN INTERNATIONAL LAW 128 (Recueil Des Courts, 1964, A. W. Sijthoff, Leyde) [hereinafter MANN-1].

[21] MANN-1 *supra* note 20, at 39 and 49 and F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 12 (1990, Clarendon Press, Oxford) [hereinafter MANN-2]. This test or principle is derived from the totality of the sources upon which, according to Article 38 of the I.C.J. Statute, international law rests, *id.* 17. The international jurisdiction to adjudicate is not a separate type of jurisdiction, but merely an emanation of the international jurisdiction to legislate, that is, a State's right of regulation is exercised by legislative jurisdiction, which includes adjudication. It follows that both aspects of jurisdiction are co-extensive, *id.* 51. The customary law and general principles of law relating to jurisdiction are emanations of the concept of domestic jurisdiction and its concomitant, the principle of non-intervention in the internal affairs of other states, IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 309 (6th Edition, 2003, Clarendon Press, Oxford) [hereinafter BROWNLIE].

[22] BROWNLIE *supra* note 21 at 297.

- there is a substantial and bona fide connection between the subject-matter and the source of the jurisdiction
- the principle of non-intervention in the domestic or territorial jurisdiction of other states is observed
- a principle based on elements of accommodation, mutuality, and proportionality is applied. Thus, national resident abroad should not be constrained to violate the law of the place of residence."

These principles are also used by the American Law Institute in its Restatements (Third) of Foreign Relations Law, which aim to set out rules for international law on jurisdiction.[23]

In the U.S., it is now well-established case law that a website with a content equal to yellow pages or advertising in national magazines cannot be regarded as targeting any particular jurisdiction.[24] For a commercial website to give basis for exercise of personal jurisdiction a plaintiff has to show evidence that, the defendant has done business with a person in the forum where the court is located. In a similar fashion, the European Union in relation to the Regulation on Jurisdiction and Enforcement[25] has stated:

"The Council and the Commission point out in this connection that for Article 15(1) (c) to be applicable it is not sufficient for an undertaking to target its activities at the Member State of the consumer's residence, or at a number of Member States including that Member State; a contract must also be concluded within the framework of its activities. This provision relates to a number of marketing methods, including contract concluded at a distance through the Internet... [T]he mere fact that an Internet site is accessible is not suffi-

[23] Especially the rules in §§ 402-403, 421 and 431. See SPANG-HANSSEN-2 *supra* note 3, chapters 25-28.

[24] Unlike newspaper, mailing, radio, television and other media containing advertisements and solicitations, most Internet advertisements and solicitations are not directed at a specific geographic are[a] or marke[t]; to the contrary, advertising on the Internet targets no one in particular and everyone in particular in any given geographic location, *Millennium Enterprises, Inc. v. Millennium Music, LP*, 33 F.Supp.2d 907, 914 (D.Or. 1999).

[25] E.U. Council Regulation 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (into force on March 1 2002), O.J. L 012, 16/01/2001 pp. 0001 – 0023, which now also covers Denmark pursuant to a Parallel-treaty, see above footnote 10.

cient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. In this respect, the language or currency which a website uses does not constitute a relevant factor."[26]

Some American courts has further required evidence showing more that a few fortuitous sales to the forum of the court.[27]

The American courts uses a federal "minimum contacts test"[28] that to a certain extent is equal to the link or point of contact that is used in international law on jurisdiction. Many American courts uses - outside cases involving tort[29] - a "Als Scan Test"[30] built upon a "Zippo Gliding Scale Method"[31] over a person outside of the State when that person:[32]

- directs electronic activity into the State
- with the manifested intent of engaging in business or other interactions within the State, and

[26] Joined declaration issued by the European Parliament and Commission at the time the Regulation was passed - Statement on Articles 15 and 73 at <http://europa.eu.int/comm/justice_home/unit/civil/justciv_conseil/ justciv_en.pdf>, reprinted in SPANG-HANSSEN-2 *supra* note 3, at 564-566.

[27] SPANG-HANSSEN-1 *supra* note 13, at 198-199 and 336-338.

[28] SPANG-HANSSEN-1 *supra* note 13, at 27-36.

[29] The "effect test" endorsed by the Supreme Court in *Calder v. Jones*, 465 U.S. 783, 788-89 (US 1984) "is used when the harm allegedly suffered by plaintiff sounds in tort," *Northwest Healthcare Alliance inc. v. Healthgrades.com Inc*., 50 Fed.Appx. 339, *certiorari denied* 123 S.Ct. 1909 (US April 28, 2003, No. 02-1250). The "Effect Test": "(1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered – and which the defendant knows is likely to be suffered – in the forum state," *Core-Vent Corporation v. Nobel Industries AB*, 11 F.3d 1482, 1486 (9th Cir. 1993).

[30] *Als Scan, Inc. v. Digital Service Consultants, Inc*., 293 F.3d 707, 712-714 (4th Cir. June 2002), *certiorari denied* 123 S.Ct. 868 (U.S. Supreme Court, January 13, 2003 - No. 02-463). See further this book Chapter 4 about the Zippo Sliding Scale-Method.

[31] The Zippo-court concluded 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, *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*., 952 F.Supp. 1119, 1122-1124 (W.D.Pa. 1997)

[32] See also above chapter 4.

- that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

It should be pointed out, that as for the E.U. Regulation on jurisdiction the language[33] or currency used on a website are not "relevant factors" when deciding the jurisdictional question pursuant to the Joint Statement to the Regulation.[34]

The content of domain names[35] should neither be a relevant determinator

[33] Otherwise Danish professor Mads Bryde Andersen that holds the use of the Danish language on a website - which is significant related to the territory of (South)Denmark - imply a nearly indispensable presumption that the website is targeting Danish consumers, MADS BRYDE ANDERSEN: IT-RETTEN [(Danish) IT law] section 23.1.b page 921-922 (Forlaget IT-retten [IT-law Publishing], Copenhagen, 1. Ed. - ISBN 87-988580-0-0-9) [hereinafter BRYDE ANDERSEN], also at <www.it-retten.dk> (in Danish). - However, a Danish languaged website can have been made by the "Danish town" Solvang in California or by associations of Danes living abroad and pointed at these abroad and locally placed Danish languaged persons, rather than especially targeting Denmark.

[34] Certain search-engines can with use of plug-ins be configured automatically to translate foreign languaged websites to the consumers preferred language.

[35] A domain name lacks a physical existence. The mere fact that it is registered through a corporation that happens to carry on business in Toronto does not give the domain name a physical existence in Ontario. A domain name is still simply a unique identifier for a particular internet site located on a particular computer. That computer may be located anywhere in the world and be unrelated to where the domain name is registered, *Easthaven Ltd. v. Nutrisystem.com Inc*., 2001 CarswellOnt 2878 para 25 (Ontario Superior Court of Justice, August 2001 - 00-CV-202854). *Hotelkette "Maritim"* (Germany) *v. Hotel Maritime* (Copenhagen) (Landgerecht Hamburg, 16. Chamber 3. August 2001- Az: 416 O 294/00) *affirmed by* Hanseatisches Oberlandsgericht Hamburg (3. Zivilsenat, 2. May 2002 - Az: 3 U 312/01) (Danish hotel had registered the domain name "hotel-maritime.dk", which it used for advertising of its hotel-business "Hotel Maritime" in Copenhagen. The website contained amongst others information in German. A German company, Maritim Hotelgesellschaff owned the E.U registered trademark under hotel businesses "Maritim" and claimed in a German court, that the Danish hotel through the use of the domain name infringed its trademark. The Danish hotel only had business in Denmark. The German court held that the violation of the trademark was happening in Denmark as the hotel-service could only be fulfilled in Denmark. This violation had no relevance in Germany. The use of the German language on the website was not sufficient evidence as for actual sales to Germany. The

for the question of personal jurisdiction,[36] as any domain name, for example ".dk",[37] can be used from serves abroad by foreigners that do not have any connection to Denmark besides that they have bought the domain name because it was low-priced, or because parts of the name consisted of a description or a indication, which the foreigner could use in his business or other activity. Danish domain names can be sold to anybody[38] and without any demand for the purchaser to aim its activity at Denmark or observe Danish law.[39]

decisive was whether there had been sales in Germany, which the court did not found was shown), at <http://www.jurisweb.de/jurisweb/cgi-bin/j2000cgi.sh> (visited March 2004, password required).

[36] U.N. REPORT OF THE WORKING GROUP IV ON ELECTRONIC COMMERCE of 19 May 2003 (A/CN.9/528) para 81 suggests at the "sole fact that a person makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in such country," which has become part of article 7 of a Preliminary draft convention, see Legal aspects of electronic commerce of 26 August 2003 (A/CN.9/WG.IV/WP.103) <http://www.unicitral.org /en-index.htm> (acn9-528-e.pdf & wp-103-e.pdf). The majority of US courts hold that simply placing the name of trademark on a website is not enough to show that a defendant has intentionally targeted the forum state. To hold otherwise would subject millions of internet users to suit in the state of any company whose trademarked name they happen to mention on a website, *HY Cite Corporation v. Badbusinessbureau.com, L.L.C.*, 297 F.Supp.2d 1154, 1166 (W.D. Wisconsin, Jan. 8, 2004) at *11.

[37] Some courts in the U.S. has claimed that websites under ".com", ".net" and ".org" should be regarded as belonging to the U.S. and thus imply the necessary minimum contact that allows exercise of personal jurisdiction by American courts. This point of view is hardly accepted by the large amount of foreign owners of domain names under these generic IP-addresses, which the inventors of the Internet globally divided the IP-addresses into.

[38] *Bonnier Media Limited v. Greg Lloyd Smith*, [2002] E.T.M.R 86, para 3-4, 2003 S.C. 36 (Scottish Outer House, July 2002 - A1334/02) (A domain name case. Noting that once a domain name has been allocated, the user can assign it to another person).

[39] BRYDE ANDERSEN *supra* note 33, at 919, section 23.1a., but differently *id*. at 921-922, section 23.1.b, where Danish professor Mads Bryde Andersen holds, that when a homepage is under the .dk-domaine name system there exists a presumption for the webpage targets Danish consumers. He holds this presumption is also to be used even though the web-advertising cover a hyperlink, which connects the user to a server that is located in foreign jurisdiction. Further he holds a similar presumption for use of Danish law when the homepage is under a gTLD (com, .net or .org) or a ccTLD, that

The decisive must be, that the activity - not a (fortuitous) search-name (domain name) for the IP-address - on the website especially targets Denmark and does not contain access-preventions against persons that stay in Denmark, for example does not recognize persons with Danish zip-codes (user key type in), or computers that are hooked up to servers in Denmark (geolocation-technology).[40]

It must also be decisive whether a website's user-terms states that it only is aiming a special territory, or whether a homepage requires a positive acceptance of the user-terms to get further into the website.[41] In so far a foreign website content a hyperlink to other websites, it has to be determined whether the latter contain new user-terms.[42] For example, the hyperlink on

contains associations to words, which is part of the Danish language (i.e. .nu or .tv), if the homepage contains information in Danish.

[40] Differently Danish professor Mads Bryde Andersen that presumes the foreign business has overview of what the users in the world do on its online website, even though the business does not have to participate in cases of pure bits-transmission (downloading together with payment), BRYDE ANDERSEN *supra* note 33, at 759, section 19.2.a - However, if the consumer uses an electronic agent, the consumer need not be logged on to his computer, since the consumer-agent already will be somewhere in Cyberspace (can move between fortuitous servers on the international computer networks), where the agent can negotiate, purchase and so on on behalf of the consumer.

[41] *ProCD, Inc v Zeidenberg*, 86 F 3d 1447, 1452 (U.S. Appeals Court for 7th Cir 1996) (The user was bound by the online agreement, since he "had no choice, because the software splashed the license on the screen and would not let him proceed without indicating acceptance"). Online agreement also upheld in *CompuServe v Patterson*, 89 F.3d 1257, 1263 para 7 (U.S. Appeals Court for 6th Cir 1996) (User was non-consumer).

[42] As for forum selection agreements in Denmark, see Rpl. § 245. Danish law makes certain requirements to the validity of forum selection agreements, which can be entered either by a statement or implied and either in writing or oral. The agreement has to be clear and concern a specific legal matter or an already existing dispute. Forum selection agreements can only be made in dispositive cases. In case a Danish court by agreement is deprived competence, there will probably be required a close connection to a foreign country and a reasonable interest for the choice of forum, ALLAN PHILIP *supra* note 5, at 102, CIVILPROCESSEN *supra* note 15, at 132-137, BETÆNKNING NR. 1052 AF 1985 OM RETTERNES STEDLIGE KOMPETENCE I BORGERLIGE SAGER [Report no. 1052 of year 1985 on the jurisdiction of courts in civil cases] 62 and 79 [hereinafter BET 1052/85], Ketilbjørn Hertz, *Værnetingsaftaler i internationale forbrugeraftaler*

[Forum selection in international consumer agreements], JOURNAL OF LAW PART B 1999B.39ff. **From Danish case law**: *Tweede Algemeene Verzekering Maatschappij (Netherlands) v. Forsikringsaktieselskabet "Danske Atlas"*, UfR 1921.622 H (Supreme Court of Denmark 2 May 1921)(A reinsurance contract between a Dutch company and a Danish company stated that all disputes concerning the contract should solely be regulated and be decided by the ordinary court of Amsterdam pursuant to Dutch law. Accordingly, a case brought in Denmark by the Dutch company against the Danish company was dismissed), *Firma Karl O. Helm v. H.A. Hagbarth A/S*, UfR 1962.247 H (The Maritime and Commercial Court in Copenhagen 11 October 1961)(Hamburg as choice of forum in an order-acknowledgement and invoice from German company approved), *ASX 265 A/S v. Ulrik Flening*, UfR 1975.428 H (Supreme Court of Denmark 24 March 1975)(Standard-clause choosing Swedish courts was invalid as the dispute lacked link to Sweden), *Steen Sahl Christensen v. K/S CEVO-Invest X*, UfR 1997.985 Ø (Eastern Appeal Court 11 April 1997)(The Maritime and Commercial Court in Copenhagen can only be chosen as forum for cases, where by evidence special knowledge to maritime or commercial issues are of (vital) importance for the decision, as cases otherwise belong to the ordinary courts), *Jørgen Jakob Hempel v. I.C.H. Industrial and Commercial Holding A/S*, UfR 1982.441 H (Supreme Court of Denmark 25 March 1982)(Switzerland as forum choice in a executive-employment contract excluded lawsuit in Denmark concerning claims based on the executive-employment contract), *Felixstowe Dock & Railway Co. (England) v. Investorgruppen Danmark K/S and A/S Det Østasiatiske Kompagni*, UfR 1990.597 H (Supreme Court of Denmark 14 June 1990)(Held England as forum choice in a contract on a container-terminal in England was not only for the advantage of the plaintiff; and the clause covered also claim for damage that defendant's vessel had caused while using the container-harbor covering the contract. Also mentioned Article 17(4) of the Brussels Convention), *Sabroe Refrigeration A/S and Sabro Refrigeration Inc. (USA) v. Lars C. Matthiesen*, UfR 1996.937 H (Supreme Court of Denmark 30 April 1996) (Choice of the Maritime and Commercial Court in Copenhagen as forum in an employment contract could not set aside Rpl. § 9(6) 6 (of 1986). Thus, a case brought before the Maritime and Commercial Court in Copenhagen was dismissed - fact mentioned in decision of 28 August 1995 by the Supreme Court of Denmark in UfR 1995.898 H) , *Con-Mec A/S v. Fournais Handels- & Ingeniørfirma A/S*, UfR 1998.728 SH (The Maritime and Commercial Court in Copenhagen 18 February 1997) (Danish supplier had to a Danish buyer in its invoice referred to the terms of delivery of its German sub-contractor. The forum clause was set aside since the clause was unusual between two Danish companies and had not been explicated noted by the plaintiff, the Danish supplier). *Landsbanki Islands Lögfrændingadeild v. Akzo Nobel Chemicals B.V.* (the Netherlands), UfR 2002.290 H (Supreme Court of Denmark 6 November 2001) (The Maritime and Commercial Court in Copenhagen as forum choice was

Yahoo.com to Yahoo.dk result the user is transferred from American to Danish user-terms. In this case, the existence of the hyperlink on the American site to a Danish site should imply, that personal jurisdiction should be allowed over the American site. In itself, a hyperlink should not be a factor that allows use of Danish jurisdiction rules. The decisive must - as always - be that the activity - not a (fortuitous) hyperlink - on the website especially targets Denmark. Some scholars have noted, at that is "good netiquette" using hyperlinks to alternative websites - at least the existence of such a hyperlink on a foreign website to a Danish website in that case should not allow Danish jurisdiction.

It should not be forgotten, that hyperlinks are the technical fundamental that connects the separate webpages to what is named the World Wide Web. Thus, one cannot split hyperlinks into specific jurisdictions [43] and this was precisely the aim of its constructor, Berners-Lee.[44]

Finally is should be pointed out, that several newer American court-

valid). *Spedition Network ApS v. Klaipedoes Litranspedas* (Lithuania), UfR 2001.2103 SH (The Maritime and Commercial Court in Copenhagen 20 June 2001)(Clause on arbitration at a Danish court did not imply forum choice in Denmark), *Firma Electronic v. Konkursboet Stenløse Plastic*, UfR 1978.876 H (Supreme Court of Denmark 2 October 1978)(Forum clause not valid against a bankrupt estate), *CEAG Sicherheitstechnik GmbH v. Eksportkreditfonden EKF*, UfR 2001.1529 H (Supreme Court of Denmark 19 April 2001)(Germany chosen as forum was valid against the Danish Export Credit Fund, which had substituted a bankrupt estate), *Bejle Gardiner I/S under konkurs v. Eilermark A.G.* (Germany), UfR 1978.575 V (Western Appeal Court 14 March 1978)(Terms of buy and delivery containing a forum clause choosing Westfalen, Germany, between a German supplier and a Danish partnership was not binding for the creditors of the Danish partnership and thus the bankrupt estate in a case about invalidation - even though the forum clause was determining for the question of the lawsuit about the obligations of the buyer and seller pursuant to contracts of delivery).

[43] *British Telecommunication Plc v. Prodigy Communications Corp*., 217 F.Supp.2d 399, 406 (S.D.N.Y., Aug. 2002) (Rejected plaintiff had patent on hyperlinks. The functionality of hyperlinks is thoroughly described in the decision). A Dutch appeal court has characterized hyperlinks "as merely a road marker on the Internet," *Scientology v. Dataweb B.V. & Karin Spaink* (Court of Appeal of Hague, Chamber M C-5, No. 99/1040, 4 September 2003) at <http://www.xs4all.nl/uk/news/overview/ scientology.pdf> (visited September 2003).

[44] <http://www.ibiblio.org/pioneers/lee.html> (visited April 2003).

decisions and reports holds that there does not exist - at least for the time being - filter or geolocation software,[45] which works to in such a degree that it can be used (by courts or legislators) as a decisive for the question of jurisdiction. One of the constructors of the basic (IP/TCP) protocol for the Internet has stated that it was a fundamental requirement that no hazards or hindrance could be put into the Net.[46]

******

9.1. Chapter 22 of the Danish Civil Procedure Code

As for Chapter 22 of the Danish Civil Procedure Code[47] (Rpl.) on the competence of the courts and cases where a (procedural[48]) foreign non-E.U. person[49] make bit-transmission on international computer network without having any tangible effects in Denmark, the following jurisdiction-rules is not usable: §235 (require residence in Denmark), §236 (require Danish citizenship), §238 (require main office or head manager in Denmark), §§239-240 (defendant is the Danish State or a Danish municipality), §241 (require real estate in Denmark), §246a (require vessel), §247 (require special convention-

[45] SPANG-HANSSEN-2 *supra* note 3, section 31.2.2.1.

[46] Vinton Cerf to Matt Berger, *Yahoo case raises issue of Internet Borders*, UPSITETODAY, 3 November 2000 <http://www.upsite.com> (visited November 2000).

[47] Unofficial translation by Henrik Spang-Hanssen into English in Appendix 7.

[48] A person is procedural foreigner if he by residence or stay has a stronger link to foreign countries than Denmark. Citizenship is without any importance, BET 1052/85 *supra* note 42, at 18.

[49] "Foreigner" are: (1) a person living abroad without residence in Denmark, (2) a person that stay in foreign countries without link to the Danish territory or without previous residence in Denmark, and (3) a person that stay in Denmark with residence outside Denmark, KARNOV LOVSAMLING [Karnov statute book] Vol. 3 note 999 (17. Ed., 2001). See also Folketings Tidende [Official Journal of Danish Parliament - hereinafter F.T.]] 1985-86, Supplement A, column 2940. BET 1052/85 *supra* note 42, chapter 4 on international jurisdiction-rules outside the territory covered by E.U. jurisdictional rules.

rule exist[50]).

9.2. The Seven Prongs, A-G.

On the other hand, the following articles might be used,[51] see Rpl. §246:[52]

A. The place from where a natural person's business is done, and the suit

[50] *1st Mover Aps* (Denmark) *v. Direct Hedge S.A.* (Switzerland), UfR 2002.1370 Ø (Eastern Appeal Court 7 March 2002) (Dispute covered by the Lugano Convention Case concerned payment for making a web site on the Internet).

[51] The so-called supplementary or exception jurisdiction-rules (supplerende eller undtagelsesværneting) which are not based on defendant's residence or place of stay, confer statement of the Minister of Justice to bill no. L. 118 on amendment of the Civil Procedure Code et al., F.T. *supra* note 49, 1985-86, Supplement A, column 2940.

[52] Rpl. § 248 subsection 1 requires a Danish court ex officio to ensure the case is brought before the correct forum. If the defendant does not raise any objection against the courts competence in first statement of defense, the court will regard itself as having jurisdiction. Subsection 2: If the lawsuit is filed at a court that does not have jurisdiction or cannot deal with one of the claims, if possible the court shall transfer the case or the claim to the correct court. A decision of transfer is done in the form of a court order. If transfer is not allowed, the court shall dismiss the lawsuit by a judgment. See CIVILPROCESSEN *supra* note 15, at 121. The rule in §248 subsection 1, 1 sentence is without any influence, confer to second sentence dealing with the situation where defendant makes no objection to the forum, compare to §232. Transfer is only done within the geographic area covered by the Civil Procedure Code that is not to Greenland or other E.U. Member states. In case of transfer, it is probably the time when the suit originally was filed that is determining for the question of jurisdiction, if defendant has changed venue in the meantime. It is a condition for the court to be competent pursuant to § 248 subsection 1, 2. sentence that defendant either makes a first statement of defense or shows up in first preliminary meeting, KARNOV LOVSAMLING [Karnov statute book] Vol. 3 note 1019 (17. Ed., 2001). *Alfa-Bank v. S*, UfR 2000.1635 Ø (Easter Appeal Court 6 April 2000)(Attorney's objection against the forum allowed, even though defendant himself in a first statement of defense only had claimed acquittal for the subject matter, since no preliminary meeting had been held in the case that until then only had been handled in writing pursuant to Rpl. §352, wherefore the court had had no opportunity to give guidance to the defendant, which had had no legal adviser at the time of first statement of defense, and the claim of wrong forum was made on behalf of defendant before the time of the reply-statement).

concerns the business, Rpl. §246 subsection 1, confer Rpl. §237.

B. Cases, against corporations, associations, private institutions and other kinds of organizations that can be a party to an action and that do business outside the "home jurisdiction", and where the suit concerns the business, can be brought before the court where business is done, Rpl. §246 subsection 1, confer Rpl. §238 subsection 2.
C. Cases concerning contracts, at the place where the obligation or responsibility on which the claim is based has been or should be fulfilled, § 246 subsection 1, compare § 242 subsection 1
D. The place in Denmark where the breach of law took place, Rpl. §243.
E. The consumers "home jurisdiction", that is the court including the residents of the consumer, if a special offer or advertising was given in Denmark before an agreement was done and the necessary actions for the fulfillment were made by the consumer in Denmark, Rpl. §246, subsection 1, 2. sentence.
F. If none of the above alternatives can be used and the suit concerns financial circumstances the case can be brought at the place where a natural person stayed at the time of service of process, Rpl. §246 subsection 2.
G. If none of the above alternatives can be used and the suit concerns financial circumstances the case can be brought at the place where the natural or other legal persons at the time for the filing of the suit has property, or if the claim concerns property, at the place where the property is at the time for filing the suit, Rpl. §246 subsection 3.

9.2.1. Prong A: § 246 subsection 1, compare § 237

Lawsuits against natural persons who run a business can be brought in the jurisdiction of the permanent place(s) of the business when the lawsuit concerns the business

The rule can be used on any business that is done by a self-employed[53] per-

[53] KOMMENTERET RETSPLEJELOV [Commentary to the Civil Procedure Code] Vol. I page 367 (6. Ed., DJØF Publishing 2000 - 87-574-6855-9) [hereinafter KOM RPL-I] and CIVILPROCESSEN *supra* note 15, at 101-102. *Kreativt Center A/S v. Karen Margrethe*

son[54], which is a foreigner with residence out an E.U. Member State.[55] It deals with disputes concerning obligation in or outside contracts related to the business.[56]

The provision does not require that the natural person that owns the business have residence in Denmark.[57] The decisive time for the jurisdictional question is the time of filing the lawsuit in court.[58]

If the personal business is done from different permanent places then the provision can be used for each of such places.[59]

On can question whether it is a requirement for the use of §237 that the business has a physical location in Denmark. Danish professor Mads Bryde Andersen is of the opinion that the starting point for "the place" (and thus the jurisdictional question) from which a self-employed person does his business is the business physical place in shape of an office where employees are lo-

Reiff, UfR 1984.324 V (Western Appeal Court 23 January 1984) (Held co-founder of a corporation under registration, which latter had done business, had not done business) and *Dansk-spansk vinimport D.S.V. A/S under konkurs v. Anselm Mayrs dødsbo* (Switzerland), UfR 1985.709 Ø (Easter Appeal Court 11 March 1985) (Bankruptcy estate directors' liability against a now dead foreign main shareholder and member of the board of directors. Held there was no non-contractual liability and neither property that could be used as base for jurisdiction in Denmark), *Lund-Hansen Advokatvirksomhed ApS v. Benedikte Moeskær,* UfR 2002.1676 Ø (Easter Appeal Court 15 April 2002) (Case concerning payment of fee for legal advice about a tenanted property could pursuant to §237 be brought at the place of the business, that was the place of tenanted property).

[54] Patent Act §64 subsection 2: Applicant and patent holders not residents in Denmark are regarded having "home jurisdiction" in Copenhagen in suits brought pursuant to the Act, KOM RPL-I *supra* note 53, at 367 note 2.

[55] ALLAN PHILIP *supra* note 5, at 91.

[56] ALLAN PHILIP, DOMSKONVENTIONEN: EF-IP II, VÆRNETING-TVANGSFULDBYRDELSE AF FREMMEDE RETSAFGØRELSER (1986) s. 144 (DJØF Publishing, Copenhagen 1986)

[57] *Orla Stenhøj v. Eksportkreditrådet*, UfR 1982.220 V (Western Appeal Court, 23 November 1981)(D living in Flensburg, Germany, and having a registered consultant business in the Danish town Kruså where he had rented an office, had only had a few assignment in Denmark and only issued one invoice in Denmark. Besides this business, a firm in Flensburg employed him. Held D on basis of the facts of the character and size of his business did not do business in Denmark).

[58] KOM RPL-I *supra* note 53, at 363.

[59] KOM RPL-I *supra* note 53, at 367 note 6 and CIVILPROCESSEN *supra* note 15, at 101-102.

cated and business is performed.[60]

Report no. 1052 of year 1985 on the jurisdiction of courts in civil cases (the basis for the present Danish jurisdictional provisions) points out, the expression "hvorfra virksomheden udøves" ["permanent place(s) of the business"] normally covers the place, where the management is, whereto correspondence is addressed, and where contracts is concluded.[61] However, this interpretation does not rule out the possibility of using the provision where no physical place in Denmark of the business can be pointed out. The Report requires solely that the business has such a link to a certain location that the business can be said to be done from that place.[62]

If one follow the restricted interpretation as Mads Bryde Andersen suggests there will be no jurisdictional provision in Denmark for pure online businesses as such businesses precisely is characterized by not having any physical place (by being in Cyberspace). Such a gab in the Danish jurisdictional rules would be bad when one considers the extent the Danes uses the Internet.[63]

According to the "Ordbog over det Danske Sprog" [the Danish equivalent of the Oxford English Dictionary][64] the word "sted" [~ "place"] covers: (commonly) a part of space, fixed location, place or point, where somebody or something is located on a shorter or longer period; (1.3) about locality, place where something is or will be done; (2) a larger or smaller part of space or some other area; frequently a point in the terrain, locality (without though of premises); (4) a relative limited, restricted part of a greater whole; (6) a place, room that can contain a person or thing, or a place where a person or

[60] Further, he notes that if the place of the physical server for the website should be the decisive, the requirement of a "place" would have to be terminated, BRYDE ANDERSEN *supra* note 33, at 919-920, section 23.1.

[61] BET 1052/85 *supra* note 42, at 14 and BETÆNKNING NR. 368 AF 1964 OM BEHANDLING AF SØSAGER [Report no. 368 of year 1964 on Maritime Cases] page 28.

[62] BET 1052/85 *supra* note 42, at 14.

[63] Taking account of the base for and the very liberal case law on Rpl. §246 subsection 3 (the "Goods-jurisdiction-rule") there does not seem to be any reason to make any restrictive interpretation.

[64] DET DANSKE SPROG- OG LITTERATURSELSKAB: ORDBOG OVER DET DANSKE SPROG [The Danish Language and Literature Society: Dictionary on the Danish Language] (2. Ed. Gyldendal Publishing, Copenhagen 1969).

thing belong.

These definitions and the Report's attitude as previous mentioned does not exclude that a pure online business steadily done over a longer period through a website owned by a foreigner should not be covers by the provision in question here.[65] If the business website is "stationary" and continuously exists on the international computer networks the business can hardly be said to be done from (constantly) changing places, which would hinder the use of the provision.[66]

Taking into consideration the large and growing part of online commerce, for example of computer games that often is delivered by download from the vendors website, it is more than likely that foreign businesses continuously will make sales to Danes through business websites (maybe even in the Danish language), which are made and owned by natural persons in foreign countries.

The provision is written at a time where business sales were done to customers through an office in Denmark.[67] The Internet has made it possible to do business in Denmark only with use of a website through which correspondence can be done and contracts concluded.

Further, when one take into consideration the sometimes exorbitant interpretation of other parts of §246 that catch foreigners without a physical location in Denmark, there should be no reason to hinder § 246 subsection 1,

[65] This suit best the base for the new wording of the Act on Certain Consumer Agreements that does not require any meeting to be held, see further below.

[66] CIVILPROCESSEN *supra* note 15, at 101 and BET 1052/85 *supra* note 42, at 14 and 74, *Irvin B. Gold v. Chevron Petroleum Company of Denmark*, UfR 1989.969 Ø (Easter Appeal Court 20 June 1989) (Defendant was a branch of an American parent company, which had been defuncted, wherefore the Danish subsidiary corporation had been cancel by the Danish Register of Companies).

[67] *Bent Manholm v. Andalucia International Real Estate*, UfR 1982.266 Ø (Easter Appeal Court 27 November 1981) (Held a Spanish corporation, which had an office in Copenhagen, had done business there and therefore could be sued at that place. The business had previously distributed pamphlets to customers about the office and its Danish employees) and *Zürich Forsikring, Randers afdeling v. Hanne Enger*, UfR 1992.645 V (Western Appeal Court 14. April 1992) (Held insurance company with headquarter in Copenhagen was doing business through a branch in the Danish town Randers, whereby it also could be sued in Randers).

compare Rpl. § 237 could allow jurisdiction over a foreigner that do business only through a website. It is for the courts to determine whether the provision require a physical place in Denmark. The purpose with provision is to offer a jurisdictional forum in Denmark concerning disputes related to a business and its operations in Denmark, and if modern business is done through websites, the interpretation of the provision should cover such incidents. The final decision is for the courts to interpretate the provision or for the Parliament to make amendments to the provision.

As the provision is written it is not prohibited to interpretate the "place" - which would be in accordance with international law on jurisdiction - in such a way that the decisive is, whether the website-business has such link(s)[68] to Denmark, that it is fair to exercise jurisdiction over the foreign business.[69] It must be a total evaluation of the activity on the website toward Denmark that must be the determine, especially whether there can be done online business through the website and whether there is evidence of actual sales through the website to Denmark - a few sales from non-Danish languaged websites should not be sufficient.[70] As for international law, there should be evidence that the business through its website specially has target Denmark. It is for Denmark to decide, whether the provision can be used in one court forum in Denmark or all the forums whereto the foreign business via its website has had - more that fortuitous - sales.

[68] The issue of points of contacts and the place of effect/target of websites is more thoroughly dealt with in SPANG-HANSSEN-1 *supra* note 13, at 99-114. The Canada Customs and Revenue Agency has in the report "WHEN IS NON-RESIDENTS DOING BUSINESS IN CANADA" (November 2001) analyzed alternative points of contacts and place of effect in e-commerce, including reference to the interpretation of an OECD model law, <http://www.ccra-adrc.gc.ca/tax/technical/ecommerce-e.html> (visited January 2002).

[69] SPANG-HANSSEN-2 *supra* note 3, Chapter 32.

[70] Perhaps differently, if the premises of the Act on Certain Consumer Agreements is being followed. In the Minister of Justices remarks to the bill on amendment of rules on distance sales was pointed out, that presumingly "not much is required before a system in the sense of the Directive [E.U. 97/7 on distant sales" and that it does not matter whether the business" frequently or only sporadic makes sales-agreements by use of distant-communication", see F.T. *supra* note 49, 1999-2000 Supplement A, column 5933. Decision-making of particular restrictions in "system" is hand over to the E.U. Court of Justice, F.T. *supra* note 49, 1999-2000 Supplement A, column 5934.

On the other hand, the fortuitousness as to what server[71] a website is stored or where the domain name[72] is issued or country name used, should not be decisive. The website the consumer has seen can be a copy from a fortuitous proxy server and the domain name can be under ".dk" but be owned and used by a business anywhere on Earth since there is no requirement of using Danish law under the ".dk" domain.[73]

[71] BRYDE ANDERSEN *supra* note 33, at 919, section 23.1a.

[72] A domain name is unsuitable to locate the business, BRYDE ANDERSEN *supra* note 33, at 919, section 23.1.a. *A v. Baan Nordic A/S (tidligere Beologic A/S)*, UfR 2001.697 Ø, 698 (Easter Appeal Court 26. November 1999)(Domain name is the entrance to a certain place on the World Wide Web and can be compared with i.e. an address, a phone number or a cable address).

[73] SPANG-HANSSEN-1 *supra* note 13, at 100-118 and the Zippo sliding scale-method in chapter 4 of this book. *Göta hovrätt* (Sweden) *v. Bodil Lindqvist*, E.C.J. C-101/01 paras. 58-59, 67, 71 (E.C.J., 6 November 2003)(Case about publication of personal data on the Internet & Place of publication - Chapter IV of E.U. Data Directive 95/46 of 24/10 1995 does not lay down criteria for deciding whether operations carried out by hosting providers occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located…There is no transfer of data to a third country within the meaning of article 25 of the Directive where an individual in a Member State loads personal data onto an Internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the Internet, including people in a third country. The court noted that information on the Internet could be consulted by an indefinitely number of people in many places at almost any time; that individuals [as] author of a page intended for publication on the Internet transmits the data making up that page to his hosting provider. That provider manages the computer infrastructure needed to store those data and connect the server hosting the site to the Internet....The computers which constitute that infrastructure may be located, and indeed often are located, in one or more countries other than where the hosting provider is established, without its clients being aware or being in a position to be aware of it; and that the case did not concern activities "carried out by the hosting providers"), <www.snurl.com/2z30> (visited 11 February 2004).

9.2.2. Prong B: § 246 subsection 1, compare § 238 subsection 2

Lawsuits against corporations,[74] associations, private institutions and other kinds of organization that can be a party to an action and that do business outside the "home jurisdiction" and where the lawsuit concerns the business can be brought in the jurisdiction of the place(s) of the business

Foreign corporations and organizations without a head quarter in Denmark can be sued in the court that covers the place in Denmark where the foreign defendant has a branch if the lawsuit concerns this business. This Danish international rule on branches[75] can be used on corporations,[76] associations,

[74] JESPER LAU HANSEN, NORDIC COMPANY LAW - The Regulation of Public Companies in Denmark, Finland, Iceland, Norway and Sweden, English Translation by Steven Harris (DJØF Publishing, Copenhagen 2003 - ISBN 87-574-0794-0).

[75] The provision correspond to article 5(5) of the Brussels Convention (and article 5(5) of E.U. Council Regulation 44/2001), Comments of the Minister of Justice to Bill no. L. 1118 on amendment to the Civil Procedure Code, F.T. *supra* note 49, 1985-86, Supplement A, column 2941-42.

[76] If the opponent is not from E.U. or EØS, the jurisdictional question is decided on basis of the Civil Procedure Code, which also has a special jurisdiction for branches in §238, subsection 2. From a private law point of view, one cannot state the branch always is embrace by Danish law. This question must be determined on basis of ordinary international private law principles, ERIK WERLAUFF'S KOMMENTERede AKTIESELSKABSLOV 589-590, 593-594 (2. Ed. DJØF Publishing 2002 - ISBN 87-574-0589-1). §147 of the Danish Companies/Corporation Act states: "Foreign corporations..., which are domiciled in an E.U. member State, can do business through a branch in Denmark. Subsection 2: Other foreign companies, limited partnership and other with a similar legal status can do business through a branch in Denmark, if this is authorized by an international agreement, or if the Minister of Commerce holds that Danish companies are given the same rights in the State in question, or grant permission." *Centros Ltd* (United Kingdom*) v. Erhvervs- og Selskabsstyrelsen* (Denmark [Trade- and Companies Board]), E.J.C. case C-212/97 of 9 March 1999 para 17, 18, 24, 29 (It is contrary to Articles 52 and 58 of the EC Treaty for a Member State to refuse to register a branch of a company formed in accordance with the law of another Member State in which it has its registered office but in which it conducts no business where the branch is intended to enable the company in question to carry on its entire business in the State in which that branch is to be created, while avoiding the need to form a company there, thus evading application of the rules governing the formation of companies

private institutions and other kinds of organization that are not registered in Denmark, or which does not have a main office in Denmark,[77] but can be a party in lawsuits.[78]

The provision covers all lawsuits that concern the particular branch, if the foreign party has "home jurisdiction" outside the E.U. territory. The lawsuit must not involve the question of whether the branch exists or not.[79] Neither must the lawsuit include a question of whether the main-firm exists, as the branch is not regarded as a legal subject and the provision presume the main-firm has not been dissolved.[80]

The rule is inapplicable where the business is done from continuous changing locations, as is the case of sales through a traveling salesman or sales at fairs or other temporary points of sale.[81] Thus, the branch has to have a permanent location.

Related to international computer networks, a branch could be a Danish-languaged website translated from a foreign site, where the website is owned by persons that is located outside Denmark, if one allows a business to be evidenced by a website alone through on which is offered sales/services and with payment through the same website, see discussion above under prong A, section 9.2.1.

which, in that State, are more restrictive…does not, however, prevent the authorities of the Member State…from adopting…measure for preventing or penalizing fraud).

[77] Includes amongst others limited partnership, foundation and co-operation, KOM RPL-I *supra* note 53, at 368 note 4.

[78] BET 1052/85 *supra* note 42, at 46, 47 and 74, KOM RPL-I *supra* note 53, at 367 note 6, and CIVILPROCESSEN *supra* note 15, at 102, *Bent Manholm v. Andalucia International Real Estate*, UfR 1982.266 Ø (Easter Appeal Court 27 November 1981) (Held a Spanish company with a office in Copenhagen had done business there and therefore could be sued there. The company had to customers distributed pamphlet about the office and the Danish employees) and *Zürich Forsikring, Randers afdeling v. Hanne Enger*, UfR 1992.645 V (Western Appeal Court 14 April 1992) (Held an insurance company with headquarter in Copenhagen also was doing business at its branch in the Danish town, Randers, and thus could be sued there).

[79] KOM RPL-I *supra* note 53, at 384 note 3 and Statement no. 233 of 31 March 1924 from Law Council [Retsrådet], JOURNAL OF LAW PART B 1924B.169 (As a corporation had not been finally been registered, the provision could be used).

[80] KOM RPL-I *supra* note 53, at 369 note 9.

[81] BET 1052/85 *supra* note 42, at 46.

9.2.3. Prong C: § 246 subsection 1, compare § 242 subsection 1

Lawsuits concerning contracts can be brought at the place where the obligation or responsibility on which the claim is based has been or should be fulfilled[82]

The "performances jurisdictional rule" does not cover pecuniary claim[83] as far as this article is concern since the online business is presumed not having any "stay" in Denmark, see § 242 subsection 2, and payment of pecuniary claim under Danish law has to be delivered at creditor's place.

The provision covers only breach of the main output of the contract.[84] The characteristic for this "contract jurisdiction rule" is that it can be used even if defendant does not have any property or a fixed location of business at the place of the obligation or responsibility.[85]

[82] The rule in §242 [previously §243] is founded on The Danish Law of King Christian the 5th [Danske Lov] section 1-2-19, thus case law from before 1919 - when the Civil Procedure Code was passed - can therefore clarify the use and reach of the rule, ALLAN PHILIP *supra* note 5, at 93.

[83] That is, contractual obligation to pay an amount of money, compare BET 1052/85 *supra* note 42, at 50. *Klapmølle Dambrug (Spain) v. B.S. Forellen*, UfR 1990.408 V (Western Appeal Court 27. February 1990) (Case about damages caused by defects of some young fish, which the defendant now living in Spain had delivered in Denmark, was based on his contractual obligation and the claim was therefore not a claim of money payment in the sense of §242 subsection 2) and *Jørgen Schmidt Trading A/S v. Smedbo AB* (Sverige), UfR 1992.746 H (Supreme Court of Denmark 30 June 1992) (Claim for damages as compensation for goodwill against a Swedish supplier, which had cancelled a contract with a Danish distributor, was regarded as a claim of money payment).

[84] ALLAN PHILIP *supra* note 5, at 92 and GOMARD, FORHOLDET MELLEM ERSTATNINGSREGLER I OG UDEN FOR KONTRAKTSFORHOLD [The relation between rules of damage in and outside contracts] 100 f. (Gads Publishing, Copenhagen 1958). *Erik Mølgaard Petersen v. Helge Otto Jørgensen*, UfR 1991.779 Ø (Easter Appeal Court 3 June 1991)(Held the claim was not a claim for money payment in the sense of §242 subsection 2, since plaintiff's claim requiring specific performance (defect in floor in bought house) only had been converted to an amount of money. Thus jurisdiction pursuant to §242 subsection 1).

[85] ARNT NIELSEN *supra* note 15, at 110.

The rule covers disputes of whether a contract exists.[86] The decisive time for the jurisdictional question is the time of filing the lawsuit in court.[87] The provision is usable to both natural and legal persons.[88]

The "performances jurisdictional rule" cannot be used as for deliverance of goods, since the place of deliverance under Danish law for moveable property is the vendors place. However, the rule can be used in cases, where the foreign online business pursuant to an agreement, such as fob or franco,[89] has agreed to deliver the goods in Denmark.[90]

The provision can be used even if the contract does not require debtor's presence at the time of fulfillment and it corresponds to article 5(1) of the Brussels Convention.[91]

As for deliverance of software through bits-transmission (download) from a foreign online business-website, the decisive must be whether the buyer achieves the rights of an owner or if he only gets a license to use the software.[92]

In the first instance the provision cannot be used as the deliverance is done at the foreign creditor's residence, unless specifically deliverance has been agreed to be in Denmark, since software brought through bits-transmission

[86] BET 1052/85 *supra* note 42, at 32.

[87] KOM RPL-I *supra* note 53, at 363.

[88] KOM RPL-I *supra* note 53, at 373 note 1.

[89] That is "franco" pursuant to Danish interpretation of the law, see *Damstahl A/S v. A.T.I. s.r.l.* (Italy), UfR 2001.1039 H (Supreme Court of Denmark 15 February 2001) (Held no performance-jurisdiction (Brussels Convention Art. 5 nr. 1) in Denmark, since a franco-deliverance clause pursuant to Italian Law did not mention a place of performance, compare CISG art. 31(a)).

[90] BET 1052/85 *supra* note 42, at 77 and 49. *Spaan verpackung G.m.b.H. (*Germany*) v. Superfos Gødning A/S*, UfR 1990.295 H (Supreme Court of Denmark 12 February 1990) (Cif clause in sellers invoice hindered lawsuit in Denmark). The provision cannot be used, if the place of performance of a contract in reality only is a point where the risk changes between the parties, BET 1052/85 *supra* note 42, at 15.

[91] Comment of the Minister of Justice to bill no. 118 on amendment to the Civil Procedure Code, F.T. *supra* note 49, 1985-86, Supplement A., column 2942. On E.U., see KIM ØSTERGAARD, ELEKTRONISK HANDEL OG INTERNATIONAL PROCES- OG PRIVATRET [Electronic commerce and International process and private law] 131-160 (DJØF Publishing, Copenhagen 2003).

[92] BRYDE ANDERSEN *supra* note 33, at 784-802, sections 20.2-20.3 and Chapter 21.

must (be regarded as and) follow the rules of moveable property.[93]

[93] NØRARGER-NIELSEN & TEILGAARD, KØBELOVSKOMMENTAREN 37 (2. Ed. 1993, Gads Publishing - ISBN 87-12-01567-9), Frederik Bruhn-Petersen, *Elektronisk præstation af digitale ydelser* [Electronic deliverance of digital output] 22 (Treatise delivered at Copenhagen University April 1999 - <www.jur.ku.dk/it-ret/specialer/bruhn-petersen.pdf >). Perhaps differently *Poul Erik Bøjden v. Bikuben Girobank A/*S, UfR 1997.707 H (Supreme Court of Denmark 11. March 1997) (Held subscription for shares in an investment trust was not purchase of movables). From foreign case law on software: *Toby Constructions Products Pty Ltd v Computa Bar (Sales) Pty Ltd*, 77 FLR 377, 383, [1983] 2 NSWLR 48 (Supreme Court of New South Wales, 1983)(The court came to "the conclusion that a sale of a computer system, comprising both hardware and software, as in the present case, does constitute a sale of goods within the meaning of both the Commonwealth Act and the State legislation…I do not wish it to be thought that I am of the view that software by itself may not be 'goods'"), *Advent Systems Ltd. v. Unisys Corp*., 925 F.2d 670, 674 & 676 (3rd Cir 1991)("Hardware is the computer machinery, its electronic circuitry and peripheral items such as keyboards, readers, scanners and printers. Software is a more elusive concept. Generally speaking, "software" refers to the medium that stores input and output data as well as computer programs. The medium includes hard disks, floppy disks, and magnetic tapes… In simplistic terms, programs are codes prepared by a programmer that instruct the computer to perform certain functions. When the program is transposed onto a medium compatible with the computer's needs, it becomes software…[W]e hold that software is a "good" within the definition in the [Pennsylvania version of the Uniform Commercial Code]."), *Sct. Albans City and District Council v. International Computers Ltd*, [1997] F.S.R. 251, 264, [1996] 4 All ER 481 (English Court of Appeal July 1996)(Separate opinion by Lord Justice Glidewell: "By itself hardware can do nothing. The really important part of the system is the software…The program itself is an algorithm or formula. It is of necessity contained in a physical medium…[I]t is necessary to distinguish between the program and the disc carrying the program...In both the Sale of Goods Act 1979 sec. 61 and the Supply of Goods and Services Act 1982 sec. 18 the definition of "goods" "includes all personal chattels other than things in action and money . . ." Clearly a disc is within this definition. Equally clearly, a program, of itself, is not.), *Beta Computers (Europe) Ltd. v. Adobe Systems (Europe) Ltd*., [1996] F.S.R. 367, 377-378 (Court of Session - Outer House (Scotland), 14. December 1995)(Contracts for the supply of proprietary software were sui generis…An essential feature of an effective transaction was that the supplier undertook to provide both the medium carrying the software and the right to access and use the intellectual property embodied in it), *Horace Holman Group Ltd. v. Sherwood International Group Ltd*., 2000 WL 491372 (High Court of Justice in Queen's Bench's Division Technology and Construction Court, April 2000 - No. 1999-TCC-NO.129)(("I am not satisfied that the

In the latter instance of only buying a license to a software there should be make a distinction between cases where the software, whereto the license is issued, is downloaded to the users computer(s) and cases where the buyer only can use the software-license by connecting to the vendors server in a foreign country.[94]

In the first alternative there can be no doubt that, the seller has a continuous obligation to allow the buyer to use the software (which probably is updated from the foreign business) at the users place. Thus, pursuant to §246 subsection 1, compare § 242 subsection 1, the Danish courts at the buyers place has jurisdiction,[95] as the newest formulation of the provision does not

contract is a contract for the supply of goods in so far as it is a contract for the supply of software"), Michael Edenborough, *Computer Contract/Sale of Goods; Software "Goods" within the Sale of Goods Act 1979*, European Intellectual Property Review, 1995, E.I.P.R. 1995, 17(2), D48 (For the purpose of the VAT Act 1983, the supply of software is considered to be the supply of goods. § 61(1) of the Sale of Goods Act 1979 distinguishes between a chose in action and chose in possession, the latter being accorded protection by the Act, while the former is not), Richard Stephens, *The Legal Principles Governing the Supply of Computer Systems: Part 1*, Computer and Telecommunications Law Review, 1998, C.T.L.R. 1998, 4(2), 27-34, Phillip Johnson, *All Wrapped Up? A review of the enforceability of "shrink-wrap" and "Click-wrap" license in the United Kingdom and the United States*, European Intellectual Property Review, 2003, E.I.P.R. 2003, 25(2), 98-102, 100 (Not only did the court [in Beta Computers v Adobe Systems] consider the contract to be of a sui generis nature, being neither a sale of goods nor information…It would appear therefore that in the United States courts are accepting shrink-wrap licenses as a sale of goods.).

[94] Many software and online businesses are located in U.S. and Asia, which Denmark does not have signed any Conventions on jurisdiction and enforcement with. Neither U.S. nor countries in Asia are parties to the Rome-I Convention (E.U. Convention on the Law Applicable to Contractual Obligations of 19 June 1980, 80/934/EEC, O.J. L 266, 9 October 1980 or at <http://aei.pitt.edu/archive/00001893/01/obligations_convention_1980.pdf>.

[95] Easter Appeal Court held in the decision in *1st Mover ApS v. Direct Hedge S.A*., UfR 2002.1370 (Easter Appeal Court 7 March 2002) , after regarding developing a website was a service, that there was jurisdiction in Denmark pursuant to article 5, subsection 1 of the Lugano Convention and thus pursuant to Rpl. § 247.

require defendant's presence at the forum for the time of the fulfillment.[96] If the individual obligations of a contract has to be fulfilled a different places, there will be jurisdiction at each of these places.[97]

If the user has to connect through the international computer network to get access to the software on the vendor's server in a foreign country, the question is where the place of the fulfillment as to § 246 subsection 1, compare § 242 subsection 1, is. Technically the user is hindered in using the license if he cannot get a computer networks connection to the vendor's server. On the other hand could be argued, that licenser delivers the service on the buyers computer and thus at the buyers place - if a networks connection was established. At this place should be noted an ancient doctrine in international law states plaintiff must sue at the place of the defendant.[98] This combined with the software being located outside Denmark points in favor of rejecting the use of the "performances jurisdictional rule" is such cases. In practice the answer will most often have been solved in the license agreement, which agreement in online business is entered by (positively) accept of terms on the website that often pinpoints a court as forum for disputes.[99]

[96] Allan Philip presumed this was the case as for the previous wording of the provision. It is required neither that defendant is in Denmark at the time for filing the suit or at the time of service of process, ALLAN PHILIP *supra* note 5, at 92.

[97] BET 1052/85 *supra* note 42, at 32.

[98] Actor sequitur forum rei, Plaintiff has to submit to the defendant's court.

[99] Click-wrap or Click-web terms, see *ProCD, Inc v Zeidenberg*, 86 F 3d 1447, 1449, 1452 (U.S. Appeals Court for 7th Cir 1996), *CompuServe v Patterson*, 89 F.3d 1257, 1263 para 7 (U.S. Appeals Court for 6th Cir 1996) and SPANG-HANSSEN-1 *supra* note 13, at 80-94. On so-called browse-wrap agreements see *Specht v Netscape Communications Corp*, 150 F.Supp.2d 585 (S.D.N.Y., July 2001) *affirmed by* 306 F.3d 17 (U.S. Appeals Court for 6th Circuit October 2002) and Henrik Spang-Hanssen, *Online aftaler i USA* [Online agreements in the U.S.] page 103-111 (YULEX 2001, Oslo, ISBN 82-7226-060-3 or <www.geocities.com/hssph>), BRYDE ANDERSEN *supra* note 33, at 761-763, section 19.2.b. *PIL-Pak A/S v. Crownson Fabrics Ltd*., UfR 2002.424 SH (The Maritime and Commercial Court in Copenhagen 8. November 2001) (Held the performance jurisdictional rule (= Art. 5(1) of Brussels Convention) could be used in a case where plaintiff claimed damage and a contract was unauthorized cancelled).

9.2.4. Prong D: § 246 subsection 1, compare § 243

Lawsuits concerning breach of law involving claim of penalty, damages or redress of a wrong can be brought in the jurisdiction of the location where the breach of law took place[100]

The so-called "insult or breach jurisdiction rule" covers breach of law in instances outside contract and can in such instances be used in cases about damages (on basis of culpa[101] and/or objective liability) and private prosecution.[102] Further, the provision can used in cases concerning damage related to

[100] The rule in §243 [previously §244] is founded on The Danish Law of the 5th [Danske Lov] section 1-2-19, thus case law from before 1919 - when the Civil Procedure Code was passed - can therefore clarify the use and reach of the rule. It is required neither that defendant is in Denmark at the time for filing the suit or at the time of service of process, ALLAN PHILIP *supra* note 5, at 92-93.

[101] Culpa: Failure to act as the ideal paterfamilias should.

[102] **Use of the provision denied in:** *Aktieselskabet Havnemøllen* (Aalborg) *v. Firma Je-Ba v/J. Jensen* (Glostrup), VLT 1957.292 (Western Appeal Court 15. June 1957) (Held provision cannot be used in cases where the determination depend on where there exist a valid retention of ownership until payment is made); *Trelleborg Aktiebolag* (Sweden) *v. Danske Gasværkers Tjære Kompani A/S*, UfR 1979.1033 SH (The Maritime and Commercial Court in Copenhagen 10 July 1979)(Held a case on whether defendant claimed violating use of a trademark could not be filed at the plaintiff's place as the place of a breach); *Coprosider S.p.A.* (Italy) *v. Vølund Energiteknik A/S*, UfR 1985.904 H (Supreme Court of Denmark 29 August 1985)(A case against an Italian subcontractor, which to the plaintiff other contracting party maybe had delivered imperfect curved to heat exchangers that had to be repaired for a large sum of money could not be filed in Denmark together with the case against the plaintiff other contracting party), *I.H. Nordgren* (Sweden) *v. Rederiaktiebolaget "Högmarsåo"* (Sweden), UfR 1932.645 Ø (Easter Appeal Court 11 March 1932)(In a case where a Swedish shipping company at the time of laying up the vessel in a Danish port illegal dismissed one in Sweden hired sailor, the seaman could not pursuant to Rpl. §243 section 2 file a lawsuit in Denmark against the shipping company with claim of overdue wages and cost for a done arrest of property), *Forsikringsselskabet Nye Danske Lloyd v. Stausberg ingenieurbau G.m.b.H.* (Germany), *Scan-Report A/S v. Forum Annonsbyrå AB* (Sverige), UfR 1972.1031 SH (The Maritime and Commercial Court in Copenhagen 13 July 1972)(Swedish firm send a Danish firm a letter in an envelope that was stamped "Nordic Commerce Calendar" ["Nordisk Affärs Kalender"]. The Danish firm claimed it infringed its rights as it since 1930 had published the encyclopedia "Nordic

a contract when the claim does not deal with the output of the contract.[103] Depending on the circumstances the jurisdiction-rule in §243 can be used in a case concerning product liability.[104] The provision covers slander and libel. It

Commerce-calendar" ["Nordisk Handelskalender"]. Held there was not jurisdiction in Denmark as it was not shown that was an infringement of the Danish firms rights) and *A/S N. Foss Electric v. John Shields* (England), UfR 1979.616 SH (The Maritime and Commercial Court in Copenhagen 14 March 1979)(Held an Englishman, which had been employed in the plaintiff's Danish subsidiary in England, did not have such a connection to the Danish corporation that his possible use of business secrets could be regarded as a infringement done in Denmark), UfR 1983.1038 H (Supreme Court of Denmark 18 October 1983)(Insurance company claimed reimbursement for a payment of damage against a German firm. Held no breach jurisdiction), decision commented by Supreme Court Judge Hans Kardel, *Om værneting efter retsplejelovens §244* [now 243] in JOURNAL OF LAW PART B 1984B.61, 62.

[103] BET 1052/85 *supra* note 42, at 16 and CIVILPROCESSEN *supra* note 15, at 107 note 38. Danish professor BERNHARD GOMARD, FORHOLDET MELLEM ERSTATNINGSREGLER I OG UDENFOR KONTRAKTSFORHOLD 100 [The relation between rules of damage in and outside contracts] (Gads Publishing, Copenhagen 1958) is finding support in the cases *I.H. Nordgren v. Rederiaktiebolaget "Högmarsåo"*, UfR 1932.645 Ø (see above footnote 102) and *Poul Erik Andersen v. William Mønster*, UfR 1938.1094 Ø (Easter Appeal Court 12 August 1938)(Leaseholder of a manor claimed the lessee of the hunting ground had to pay compensation for damage caused by game pursuant to the Danish Hunting Act. Held lawsuit could be filed pursuant to Rpl. §244. Remarked that even though §244 only covers breach outside contracts the provision could be used in the particular lawsuit since the obligation that was the base for the claim against the defendant had basis in the Hunting Act), and holds the cause of accident easiest can be unraveled at the place, where the accident has happened, and further make reference to traditional jurisprudence on unlawfulness. This opinion is accepted in the book review in JOURNAL OF LAW PART B 1959B.223 by A. Victor Hansen and of ALLAN PHILIP *supra* note 5, at 93.

[104] *Topdanmark Forsikring A/S v. Rentokil Svenska AB*, UfR 1996.1547 Ø (Easter Appeal Court 30 September 1996) (Jurisdiction pursuant to §243 over a Swedish manufacturer in a case where plaintiff sued for damage caused by defective). *Dow Corning International Ltd.* (Belgium) *v. Dansk Tyggegummifabrik A/S*, UfR 1986.922 H (Supreme Court of Denmark 28 October 1986)(A builder sued contractor and made third party notice to the contractor's Belgian sub-contractor for compensation for cleaning of boilers, overtime-payment and scrapping of materials caused by defects of the delivered product (sticky and sealing compound). Since the claim against the sub-contractor was based on product liability, the jurisdictional provision could be used).

also covers companies.[105]

In relation to the territorial sphere of application of the Danish Criminal Code an act is also regarded as done where the effect of the act takes place if the criminality depends of the effect,,[106] and the jurisdiction provision in §243 must be interpretated in the same way.[107] The same rule also is used in cases of violations where both the initiation of an act and the effect is done in Denmark.[108]

Thus, pursuant to §243 Denmark has jurisdiction if the act that cause the damage is done outside Denmark but the damage occurs in Denmark. In transborder cases it can be debated whether the damage is happening in State where the act was done, or the State where the effect occurred. In Danish legal theory, Danish courts can exercise personal jurisdiction as long as the place of the initiation of an act or the effect happens in Denmark.[109]

Peter Arnt Nielsen argue[110] as for cases about slander, libel, copyright infringement or business violations that it is doubtful whether it is sufficient for use of §243 that the injured person has residence in Denmark.[111] Otherwise,

[105] ALLAN PHILIP *supra* note 5, at 93.

[106] Danish Civil Penal Code of 1930 § 9: In cases where the criminality of an act depends on or is influenced by a given or intentional consequence, the act is regarded also as done at the place where the effect is or was indented to be. [I de tilfælde, i hvilke en handlings strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge, betragtes handlingen tillige som foretaget dér, hvor virkningen er indtrådt eller tilsigter at skulle indtræde].

[107] *Alfred Leopold (Norge) v. Carl Davidsen*, UfR 1940.454 H (Supreme Court of Denmark 3 April 1940)(A person with residence in Norway, which was shareholder in a corporation in the Danish town Ålborg, did from the Swedish town Helsingborg sent letters to the executive board that contained charged against on in Ålborg resident shareholder. Held the latter pursuant to Rpl. §244, compare Civil Penal Code §9, could sue in the court of Ålborg and claim punishment and damage).

[108] KOM RPL-I *supra* note 53, at 375 note 5 and BET 1052/85 *supra* note 42, at 16.

[109] O.A.BORUM, LOVKONFLIKTER: LÆREBOG I INTERNATIONAL PRIVATRET [Conflict of law: Textbook on international private law] 190 (4. Ed. 1957 Gads Publishing), ALLAN PHILIP *supra* note 5, at 93 and ARNT NIELSEN *supra* note 15, at 111.

[110] ARNT NIELSEN *supra* note 15, at 112.

[111] *Erik Fiehn v. A/B Wivefilm* (Sweden), UfR 1947.187 Ø (Easter Appeal Court 16 October 1946) (A film produced by a Swedish firm S was shown in Denmark without mentioning the name of the composer K of a melody used in the film. S should have

the last edition of Gomard: Civilprocessen points out, that a private libel action can be brought at the place in Denmark where a letter with a libel content mailed from abroad is received. This "effect doctrine" from the decision published in UfR 1940.454 H [112] is argued also available where both the initiation of an act and the effect happens in Denmark.[113]

A plaintiff that seeks personal jurisdiction pursuant to Rpl. §243 must show some evidence of the defendant being responsible for the injury.[114]

As for acts done purely online on international computer networks where anything first uploaded can be accessed be anyone connected to the Internet it should be considered whether the requirement of a close connection and reasonableness in international law on jurisdiction is achieved.

The provision in §243 is written before the Internet was developed and thus does not take into consideration that the formulation of the provision now authorize worldwide jurisdiction, because persons in Denmark has free access to Internet-actions done on the other side of the Globe that might only be intended for persons in Asia or a different cultural community, which does not consider the act as a violation.

In relation to acts done on international computer networks there should be made such a restricted interpretation of the rule in §243 that requires the act behind the violation,[115] has been aimed at Denmark[116] and that it is rea-

known this. Lawsuit for damage pursuant to the Danish Author Act could be filed in Denmark against S. However, Rpl. § 246 subsection 1 did not allow filing a claim for damage based on the showing of the film in Sweden), BET 1052/85 *supra* note 42, at 16.

[112] *Alfred Leopold (Norge) v.Carl Davidsen*, UfR 1940.454 H (Supreme Court of Denmark 3 April 1940) (mentioned above in footnote 100).

[113] CIVILPROCESSEN *supra* note 15, at 108 and BET 1052/85 *supra* note 42, at 78.

[114] Erik Siesby, *Godsværneting og sikkerhedsstillelse* [Goods-jurisdiction-rule and security], JURISTEN 1974.532, 532

[115] *Morgan Crucible Company Plc. v. A.B. Svejseteknik ApS.*, UfR 2001.432 SH (The Maritime and Commercial Court in Copenhagen 21 November 2001) (Use of a trademark in a URL-address on a business homepage constituted an independent violation). Differently *Electronic Broking Services, Ltd. England v. E-Business Solutions & Services*, 285 F.Supp.2d 686, 691-692 (D.Md, Sept. 30, 2003)(Case on trademark infringement dismissed on lack of jurisdiction - Defendant sold products and services for banking an financial entities through a website. Plaintiff, a British company, provided goods and services, including computer hardware and software, to the banking and fi-

sonable pursuant to basic international law on jurisdiction that Danish court deal with the case. [117] Maybe there should be made a distinction between incidents where the injury is related to a natural person and incidents concerning a business.[118]

As for libel-content in online newspapers[119] there should take considera-

nancial services industry under the name and owned the U.S. federal trademark "Electronic Broking Services, Limited" ("EBS"). Defendant aimed Egyptian citizens and E-Business Solutions was based in Egypt. Defendant had no physical presence in the United States, nor did defendant conduct extensive business in the country. No indication that E-Business Solutions intentionally targeted residents in Maryland through its website or directed its electronic activity into Maryland with the manifested intent of conducting business within the state. Court noted E-Business Solutions owned the "EBS" trademark in Egypt and might continue to use it in that forum and perhaps other places despite some resolution of the dispute in Maryland).

[116] *Viasat A/S and Canal Digital Danmark A/S v. A*, UfR 2002.405 H (Supreme Court of Denmark, 27 November 2002) (A was a Danish citizen with residence in Columbia. Held: §243 cannot be used in cases where the claim is an injunction. - A Dane living aboard and without any location in Denmark edited the website <www.piratdk.com> placed on a server outside Denmark. From the website could be downloaded material that was illegal in Denmark. The website was Danish languaged and concerned Danish encryption keys). Similar case in *Canal Digital Danmark A/S v. Hans Magnus Carlsson* (Sverige), UfR 2001.2186 Ø (Easter Appeal Court 26 June 2001).

[117] SPANG-HANSSEN-2 *supra* note 3, section 32.1.1.1., 32.2., and Chapter 34.

[118] When an injured party is an individual, it is reasonable to infer that the brunt of the injury will be felt in the state in which he or she resides. This is not necessarily the case when the injured party is a corporation. "A corporation does not suffer harm in a particular geographic location in the same sense that an individual does." [The "effect test" in *Calder v. Jones*, 465 U.S. 783, 789 (US 1984)] still requires that the harm be particularized to the forum state. Even if a corporation has its principal place of business in the forum state, it does not follow necessarily that it makes more sales in that state than any other or that harm to its reputation will be felt more strongly in that state. [M]erely identifying the plaintiff's principal place of business is not enough, *HY Cite Corporation v. Badbusinessbureau.com, L.L.C.*, 297 F.Supp.2d 1154, 1167 (W.D. Wisconsin, Jan. 8, 2004).

[119] Use of § 243 accepted in: UfR 1921.855 Ø (Easter Appeal Court 18 May 1921 - Kære IV nr. 203/1921) (Rpl. §244 could be used in a case against chief editor of a magazine with claim for penalty and damage caused by insults in the magazine. Lawsuit could be filed in the city where the magazine was sold) made *reference to* the case *Andelsanstalten "Vort Land" (Dansk Syge- og Ulykkesforsikringsselskab) v. Edv. Ph. Mackeprang*, UfR 1913.721 (Landsover- and Hof- and Stadsretsdomme, 27 January

tion as to the peculiarity of the Internet.[120]

In general when considering the appropriateness of the "insult or breach jurisdiction rule" should be remembered that something on a foreign website that pursuant to Danish law is a violation, very well can be legal pursuant to the laws at the place of the author of the website or the server hosting the website. If such a restricted interpretation of the rule in §243 is not taken in relation to international computer network, the provision would in reality

1913)(A case against the chief editor of a trade magazine that was claimed to contain an insulting article was filed in Copenhagen pursuant to The Danish Law of King Christian the 5th [Danske Lov] section 1-2-19 as Copenhagen was the place of publication. Noted, that the magazine's publications-place had to be Copenhagen as both printed in Copenhagen and distributed by a corporation registered in Copenhagen, even though defendant, as claimed by him, did his job from his residence in the Danish town Frederiksberg. Further remarked the defendants claim for dismissal had to be rejected, since the place of a printed publication pursuant to a special provision in the Press Act of 3 January 1851 had to be interpretated as the jurisdiction given by The Danish Law of King Christian the 5th [Danske Lov] section 1-2-19 as far libel was concerned); *Gunnar Quistgaard Vemb v. L. Egebjerg*, UfR 1957.613 V (Western Appeal Court 26 February 1957) (Held libel-case concerning some statements in a newspaper against the editor of the newspaper published in the Danish town Århus and defendant A, which lived in the Danish town Viborg, that had made the statements in a interviewed with the newspaper could not be filed in Viborg pursuant to §243 as the wrong, which plaintiff argued was made by the newspaper article, could not be in Viborg, but only in Århus, where the newspaper had been distributed).

[120] SPANG-HANSSEN-2 *supra* note 3, section 32.1.1.3. The Internet is different in one important respect from more traditional publications such as newspapers and magazines, where publishers can generally limits their exposure to liability, MATTHEW COLLINS, THE LAW OF DEFAMATION AND THE INTERNET page 307, Chapter 24 – Jurisdiction (Oxford University Press, 2001). Se also *Berezosky v. Michaels & Berezosky v. Forbes*, [2000] E.M.L.R. 643, 668, [2000] 2 All ER 986, [2000] 1 WLR 1004, 2000 WL 544123 (House of Lords, May 2000) (where "fair play and substantial justice" was considered), *Don King v. Lennox Lewis, Lion Promotions, L.L.C. & Judd Burstein* (U.S.), [2004] EWHC 168 para 15, 2004 WL 62126 (High Court of Justice Queen's Bench Division, 6 February 2004)([I]t has long been recognized that publication is regarded as taking place where the defamatory words are published in the sense of being heard or read…by analogy, the common law currently regards the publication of an Internet posting as taking place when it is down-loaded) and *Shevill v. Presse Alliance S.A.*, 1995 E.C.R. I-415, [1995] E.M.L.R. 543, [1995] I.L.P. 367 (E.C.J. Case C-68/93, 1995).

allow exercise of universal jurisdiction.

Such a regime would be contrary to international law that only allows States to exercise of universal jurisdiction in incidents where international law grants universal jurisdiction, thus a State exercise universal jurisdiction on behalf of the international community.[121] It would bring chaos on international computer network if every State could legislate about content on foreign websites and through its courts make judgments against aliens that were held to have made a violation of that State's law. As for the Danes, it would for example imply that the content of Danish websites, which were in accordance with Danish law after the liberalization of prohibition of some pornography provisions, but which sites constituted a violation in foreign countries, could be punished there. If so, Danes could be arrested at (catholic) southern European holiday-destinations or in the U.S. on basis of their websites' content, which foreigners cannot be prohibited to see (unless access is prohibited at large costs) l.[122]

For the use of §243 the determine must be that the wrong not only is felt in but also is targeted by the author toward Denmark and must presumable be limited to incidents where the alien's act neither was legal in his own State.

The schism is brilliantly illustrated in the French court decision against California Yahoo! Inc. that legally pursuant to U.S. law has allowed Americans through websites to auction goods that is felt offensive in France and where the French court has issued daily penalties of 100,000 Francs per day.[123] See further above Chapter 6.

9.2.5. Prong E: § 246, subsection 1, 2. sentence

In lawsuits concerning consumer contract, the consumer can bring a lawsuit against the persons, corporations, associations, private institu-

[121] SPANG-HANSSEN-2 *supra* note 3, at 252-254.

[122] In this context it is troubling that the U.S. find it has personal jurisdiction for circa 70 percent of what happens on the international computer networks, because circa 70 percent of the networks serves is placed in the U.S., compare the legislation related to the Patriot Act (Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism Act of October 26th 2001, 2001 PL 107-56 (HR 3162).

[123] The case is thoroughly reported in SPANG-HANSSEN-2 *supra* note 3, at 485-519.

tions and other kind of organizations at the consumers "home jurisdiction" if a special offer or advertising in Denmark was made before the agreement was entered into and the necessary actions for the fulfillment of the agreement were made by the consumer in Denmark.[124]

The interpretation of "consumer agreement" in Danish law is the decisive for the use of this provision.[125] A "consumer agreement" is pursuant to the wording of the Act on Certain Consumer Agreements[126] an agreement a businessman enter as part of his business when the other party (the consumer) primar-

[124] The provision is similar to article 13(3) of the Brussels Convention, compare confer statement of the Minister of Justice to bill no. L. 118 on amendment of the Civil Procedure Code et al., F.T. *supra* note 49, 1985-86, Supplement A, column 2943 and CIVILPROCESSEN *supra* note 15, at 122. The new E.U. Council Regulation 44/2001 of 22 December 2000 has a different content in Section 4 of Chapter 2 on jurisdiction over consumer contracts. The provision in §246 subsection 1, 2. sentence is different from the provision in § 244, which states: Lawsuits concerning consumer contracts that are not entered into by the consumer at the permanent place of the business can be brought against the business at the "home jurisdiction" of the consumer. The special consumer-jurisdiction in § 244 can be used both in cases where the business on its on initiative or has agreed to enter into an contract outside its permanent place, and in cases where the contract is entered through a phone call or by a written agreement without the consumer has contacted to the business. The Second sentence of § 246, subsection 1 makes a term of choice of forum against the consumer null and void if the term has been entered before the time of the dispute, compare BET 1052/85 *supra* note 42, at 79.

[125] Statement of the Minister of Justice to bill no. L. 118 on amendment of the Civil Procedure Code et al., F.T. *supra* note 49, 1985-86, Supplement A, column 2943.

[126] (Lov om visse forbrugeraftaler) no. 451 of 9 June 2004, amended by Act no. 824 of 25 August 2005. See also Justice Departments comments to Bill no. L 220 of 31. March 2004 and White Paper 1440 of 2004 form the Justice department's Expert panel on amendments to the Act on Certain Consumer Agreements (Betænkning om revision af forbrugeraftaleloven) <http://www.jm.dk/wimpdoc.asp?page=document&objno=71808>. See also E.U. Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, O.J. L 95, 21/04/1993 pp. 0029 – 0034 and E.U. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts O.J. L 144, 04/06/1997 pp 0019 - 0027.

ily deals outside his business.[127]

Chapter 4 of the Act on Certain Consumer Agreements[128] contains rules about obligations to give certain information and the right to annul a contract. Further it makes the following definition of "fjernsalg" [distance sales] (or rather "distanceaftaler" [distance contract][129]):[130] an contract whereby buying goods,[131] service or a continuous deliverance of goods or services when the (1) is entered[132] by use of distance communication without the parties physical meets,[133] and (2) entered as part of a system of distance contract done by the businessman.

The rules in Denmark cover Internet business.[134] In the comment to §11 of the bill on amendments in 2004 was pointed out the obvious that businesses that uses distance contracts for sales cannot only exists in Cyberspace

[127] §3. The business has the burden of proof that the contract is not a consumer-contract.

[128] Chapter 4 of the Act has to be used if the consumer makes orders by clicking on an icon on the screen or by phoning. However, the latter only if the phone number was mentioned in connection with the advertisement of the ordered product, whereas a phone number published as general information on the business's websites, F.T. *supra* note 49, 1999-2000 Supplement A, column 5954. As a phone number seldom is mentioned on the same webpage as where the product in question is published, the provision in reality seems without any significance.

[129] KARNOV LOVSAMLING [Karnov statute book] Vol. 4 note 108 (17. Ed. 2001). The definition does not require purchase of goods or that these have to be shipped. The English term in the underlying E.U. Directive 97/7 is "distance contracts".

[130] Act on Certain Consumer Agreements §4.

[131] That is physical movable article, KARNOV LOVSAMLING [Karnov statute book] Vol. 4 note 111 / 39 (17. Ed. 2001).

[132] That is, cases where only distance communication has been used until a contract is entered, F.T. *supra* note 49, 1999-2000 Supplement A, column 5934.

[133] Distance communication is by the Danish Act interpreted as any communication made without the consumer and the businessman meet physical, §4 no. 1, and preamble no. 9 of E.U. Directive 97/7. It is a requirement that the parties until the time of entering the contract only uses distance communication and thus does not meet physical, F.T. *supra* note 49, 1999-2000 Supplement A, column 5229.

[134] The Danish provision gives the consumer extended protection than article 3(1) of E.U. Directive on the protection of consumers in respect of distance contracts no. 97/7 of 20 May 1997, KARNOV LOVSAMLING [Karnov statute book] Vol. 4 note 117 and 122 (17. Ed. 2001).

and only by an Internet address.[135] However, the problem for the plaintiff (consumer) is that the physical address in the brick and mortar world may be located on the other side of the Globe and in a State, which does not have any treaty on enforcement with Denmark and thus no obligation to execute Danish court decisions (here, especially on basis of the special "consumer jurisdiction rule" in § 246, subsection 1, 2. sentence.

The Act does not exclude incidents where a consumer has used electronic agents and thus entered a contract/purchase without any human involvement on both sites. A report by American Bar Association with corporation from around the world points out that in cases where electronic agents (Bots) does the purchase it is fair to regard the "buyer" being at the place of the seller, and that the seller often will be the weak party as the consumer's Bot has the ability to compare goods and offers on the whole Net.[136] In this connection one should have in mind that the in practice overwhelming exclusion from §244 of the Danish Civil Procedure Code is the (normal) sale in stores.[137] As for electronic agents Danish Courts must decide whether Rpl. § 246, subsection 1, 2. sentence shall be interpretated restricted or follow the Danish extended wording of the E.U. Directive 7/97 on Distance Contracts.[138]

As mentioned above does the term "consumer contract" cover the buying of non-business persons if the deal is entered or arranged on behalf of the business by a businessman.[139]

[135] F.T. *supra* note 49, 1999-2000 Supplement A, column 5959. "Directive 97/7/EC of 1997 on consumers distance contracts applies to all mail order sales, including those made over electronic means," O.J. L144, 4/6/1997 P. 0019-0027.

[136] American Bar Association, ACHIEVING LEGAL AND BUSINESS ORDER IN CYBERSPACE: A REPORT ON GLOBAL JURISDICTION ISSUES CREATED BY THE INTERNET, August 2000, Business Lawyer, 55 BUSLAW 1801, 1829.

[137] KOM RPL-I *supra* note 53, at 377 note 3.

[138] On European Union Public Opinion on Issues Relating to Business to Consumer E-commerce, see SPECIAL EUROBAROMETER 60.0, Report from European Opinion Research Group EEIG (March 2004) at <http://europa.eu.int/comm/consumers/topic/btoc_ecomm.pdf> (visited March 2004).

[139] BET 1052/85 *supra* note 42, at 58. The foreign business has to fill the lawsuit at the place of residence of the consumer, compare Rpl. compare § 235 subsection 1, which cannot be deviated from by a prior agreement of choice of forum, see § 245 subsection 2.

In relation to online commerce the above-mentioned one should consider whether online auction sites are covered by the provision in Rpl. § 246, subsection 1, 2. sentence. At this point should be noted that online auctions sites deals with both sales of new goods and of used items, and that many of the vendors are manufactures that sells directly from the production line without use of retail stores. The latter could be interpretated as circumvention the consumer protection rules that are the basis for the special consumer jurisdictional rule in Rpl. § 246, subsection 1, 2. sentence. On the other hand could be argued that the consumer protection rules do not normally cover auction sales and that many of the sellers on the web auction sites are consumers themselves.

In situation where the intermediary of auction sites gain profit from advertising that are generated on the sites on which sellers offers both physical and bits-transmitted effects should not allow the use of Rpl. § 246, subsection 1, 2. sentence as the purpose of the provision - compare with Rpl. § 244 - is to catch incidents where a professional is involved in the main sale. However, an intermediary that only has income from advertising on auction sites cannot be such a professional covered by Rpl. § 246, subsection 1, 2. sentence.

The situation is opposite where the intermediary of auction sites charge a fee or gain a percentage of the auction sale. Thus, a purchase of effects from an American consumer on American Yahoo!'s auction web site could allow a Danish court to exercise jurisdiction pursuant to Rpl. § 246, subsection 1, 2. sentence, even though the American consumer as seller in his own State is bound by the terms on the Yahoo! auction site that amongst others has a forum choice clause.

Article 3(1) of the E.U. Directive 7/97 on Distance Contracts exclude auctions, including electronic auctions on the Internet, but this (default) provision is pursuant to the comment to bill departed by Denmark.[140] The latter will probably create chaos for citizens and business as the Danish departure from the default provision is a (legal) deviation of the Directive that has the main aim to strengthen the Internal Single Marked of the European Union

[140] Named §10c subsection 2 in Act no. 442 of 31 May 2000 § 1, now § 1 subsection 1 no. 4 but with an extended wording. Denmark has used the possibility in the Directive of making the rule more stringent, which however does not harmonize well with the main aim of the Directive (strengthen the similarity of the laws in the Member States).

and the Danish departure does can be written from the wording of the provision in Rpl. § 246, subsection 1, 2. sentence, but only from the comment to bill.[141] Furthermore, a re-writing of the 2000 version of §10c subsection 2 into the 2004 version, now named §2 subsection 1(4) combined with the text in §2 subsection 2 makes it more than possible for interpretate the rules on Internet auctions to cover any sale on the Internet – and even if the seller is a private citizen in another country.

Thus, foreign sellers will only reveal that the Danish rules on obligation of information in the Danish Act on Certain Consumer Agreements also has to be used for sales on auction sites if a Dane - but contrary to all other E.U. citizens - access the site if the foreigner reads the comments to the bill in Folketings Tidende [Official Journal of parliamentary proceedings (only in Danish language)]. To the ordinarily Danish citizen the situation is also an abnormality as auction sales are not (besides online auctions sales) covered by Danish law for sales and buying.[142]

It seems reasonable to limit the Danish peculiar rule as much as possible so only auction websites that are formulated in the Danish language has to fulfill the provisions on obligation of giving certain information and the right to annul a contract or hire-purchase agreement in Chapter 4 of the Danish Act, whereas Danish consumers as for auctions sites formulated in other languages than Danish must accept that the Danish special rule pursuant to

[141] Many a foreign business could make a good reasoning that he neither knew or should have known this odd and strange this exception, which can only be read from the comments to the bill, compare F.T. *supra* note 49, 1999-2000 Supplement A, column 5936 and 5956.

[142] A whitepaper on auctions on the Internet [REDEGØRELSE OM AUKTIONER PÅ INTERNETTET] of 14 March 2006 from the Justice Department summarize in section 4.4 that the Act on Certain Consumer Agreements, the Sale of Goods Act, and the Act on Agreements and Contracts apply fully in cases where a online-action-service communicates an agreement via an Internet auction between a seller, including a private seller, and a consumer. Thus, a consumer, which in this way enters an agreement, is legally protected as if the purchase had been any ordinary internet-sale. It is therefore the Justice Department's opinion that the existing law on consumer protection offers consumers a full shield when they participate in Internet auctions, at <www.jm.dk/image.asp?page=image&objno=75160> (visited April 2006).

the comment to the bill cannot be used.[143] It would have been more reasonable if the Danish special rule only covered sales of new and used effects that a business - not a foreign consumer-seller - offered through online auction sites. However, it can be hard to find evidence to determine whether the foreign auctions-seller is a consumer (private person) or a business.

It will be interesting to observe the Danish courts handling cases where the buyer is a Danish consumer that sue another Danish consumer that was selling some inheritance or stuff from a house-cleaning on an Internet auction side. Both consumers will probably be astonished by the difference between selling on a flea market on a Saturday or on an auction site on which the private selling consumer has produced all information and presented all pictures and arranged the website about the offered sales item.

The Danish Consumer Ombudsmand has in 2006 published a White Paper[144] suggesting an amendment the law so there is no doubt that all private Internet auction sales shall be covered fully by the Act on Certain Consumer Agreements. Interesting will be to see a citizens private offering to sell used items to the highest bidder not on a auction-website, but from the citizen's own homemade private website suggesting bidders to send e-mail with bids and the courts dealing with this as e-mail-correspondence or as an auction side.[145]

In relation to § 246, subsection 1, 2. sentence and Danish consumers online dealings on international computer networks the question is in what circumstances can the consumer be said to have make an application to the

[143] On can question whether Danish consumers find any rationale in a special rule that makes their sales/purchase on web-auctions-sites covered by consumer protection provisions as a businessperson, whereas the same dealings on flea markets/hay-markets only are covered by strongly limit rules.

[144] FORBRUGEROMBUDSMANDENS UNDERSØGELSE AF DANSKE INTERNETAUKTIONER of 27 February 2006 <http://www.forbrug.dk/fileadmin/Filer/Markedsf_ring_og_jura/Internetauktioner_-_Rapport_-_konklusioner.pdf> & Redegørelse om Auktioner på Internettet af 14 March 2006 (Doc. KLH40242 – j.nr. 205-709-0017) <http://www.jm.dk/image.asp?page=image&objno=75160> (both visited April 2006).

[145] If the suggested legislation goes through, Danish citizens – of which 80 % uses the Internet - must expect to be blacklisted or prevented access to the world's online auctions-websites.

permanent place of the foreign business - in casu a foreign web site of the foreign business - whereby § 246, subsection 1, 2. sentence cannot be used; respectively incidents where the foreign web site of a foreign business contain "a special offer or advertising" aiming Demark, whereby § 246, subsection 1, 2. sentence can be used.

The first alternative can be compared with incidents excluded by Rpl. § 244 on consumer agreements that are entered by personal physical enquiry at the permanent place of the business. The contrary would be that the Danish consumer jurisdiction-rule should cover a Danish tourists buying in a foreign country.

Use of Rpl. § 246, subsection 1, 2. sentence requires the foreign defendant has "a special offer or advertising" in Denmark.

Danish professor Mads Bryde Andersen remarks that the term "advertising" normally means action characterized by seeking out information but that it in relation to the Internet is hard to imagine businesses are seeking out information to consumers. He holds that an advertising from a foreign country on the Internet only can be said to target Danish consumers if there has been further active effort than just make information available on the Internet for consumers (from Denmark).[146] See further the reflection on targeting websites above.

A second condition for allowing use of § 246, subsection 1, 2. sentence is that the consumer was physical in Denmark at the time for "the necessary actions for the fulfillment of the agreement were made." The consumer must have the burden of proof that he was in Denmark. For a foreign businessperson it will be impossible to proof whether for example the consumer's laptop sent the order via a mobile phone connection while the consumer (and the laptop) was in Denmark or in an airplane/foreign country. It is in Cyberspace no big problem for a consumer to give a false place of stay, whereby use of §

[146] BRYDE ANDERSEN *supra* note 33, at 921, section 23.1.b. Unlike newspaper, mailing, radio, television and other media containing advertisements and solicitations, most Internet advertisements and solicitations are not directed at a specific geographic are[a] or marke[t]; to the contrary, advertising on the Internet targets no one in particular and everyone in particular in any given geographic location, *Millennium Enterprises, Inc. v. Millennium Music, LP*, 33 F.Supp.2d 907, 914 (D.Or. 1999)

246, subsection 1, 2. sentence is prohibited.[147] The present geotracking/localizing software is not trustworthy to the degree required by courts.[148]

9.2.6. Prong F: § 246 subsection 2

If none of the above alternatives can support exercise of jurisdiction and the lawsuit concerns financial circumstances it can be brought at the court at the place where the [natural] person stayed at the time of service of process

This exorbitant jurisdiction provision, which is subsidiary, support the possibility of universal jurisdiction as for the dealings of foreigners on international computer networks,[149] solely on the conditions that the defendant as a natural[150] person (Danish or foreigner) at the time of service of process stays in Denmark and the dispute concerns financial circumstances,[151] that is, plaintiff seeking a judgment for execution as well as action for a declaration

[147] Ketilbjørn Hertz, *Værneting i internationale forbrugeraftaler* [Forum selection in international consumer agreements], JOURNAL OF LAW PART B 1999B.39 page 39, 40.

[148] Previous Bell Labs researcher Bill Cheswick, Lumeta Corp., to Stefanie Olsen, *Geographic tracking raises opportunities, fears*, CNET News.com, 8 November 2000, at <http://news.com.com/2100-1023_3-248274.html> (visited 14 October 2003) and SPANG-HANSSEN-2 *supra* note 3, at 332-336.

[149] As Danish Law does not recognize the doctrine of forum non-convenies, Danish courts will have to deal with lawsuits that does not have much or any links to Denmark, see note 2 to *Flensburger Volksbank A.G. v. Firmaet Jacob Sørensen & Co*, UfR 1926.17 H (Supreme Court of Denmark 16 November 1925) (As defendant in Denmark had cash in banks of the amount of 212 in Danish currency, "goods-jurisdiction" existed in Denmark. It is not decisive where the passbook physical is located) and ALLAN PHILIP *supra* note 5, at 95.

[150] *A/S Svendborg Kasein v. Etablissements Freddy Baines* (Netherlands), UfR 1955.1079 SH (The Maritime and Commercial Court in Copenhagen 8 July 1955) (Service of process to the President of a foreign corporation under a stay in Denmark could not allow exercise of jurisdiction over the foreign corporation). The provision in § 246 subsection 2 cannot be used against corporations, ALLAN PHILIP *supra* note 5, at 92 and 94. CIVILPROCESSEN *supra* note 15, at 123.

[151] CIVILPROCESSEN *supra* note 15, at 123.

with a claim, which has economic value[152] and is bases on civil law.[153]

As nearly everything uploaded on international computer network can be access by everyone it is easy to image incidents where a plaintiff argue dealings of a foreign natural person on international computer networks constitute a financial circumstance bases on civil law, which incident pursuant to the provision in § 246 subsection 2 does not have to have any link to Denmark.[154]

A for the range of Rpl. § 246 subsection 2 and thus the duration and the purpose of the foreigner defendant's stay is concerned, the Minister of Justice noted in a comment to the bill[155] that not any short stay should allow the use of the provision, for example not a transit in a Danish airport.[156] The rule, that is subsidiary, cannot be used against persons in E.U. Member States[157] or persons living in States covered by the Lugarno Convention.[158]

9.2.7. Prong G: § 246 subsection 3

If none of the above alternatives (besides prong F) can support exercise

[152] In principle there is no requirement of the value of the goods, ALLAN PHILIIP-1 *supra* note 4, p 95. On the reasoning for the rule, see Erik Siesby, *Godsværneting og sikkerhedsstillelse* [Goods-jurisdiction-rule and security], JURISTEN 1974.532 and Erik Siesby, *Udlændinges værneting og udlandsdanskeres* [Foreigners jurisdiction and Danes abroad], JOURNAL OF LAW PART B 1980B.381.

[153] CIVILPROCESSEN *supra* note 15, at 123. *Pakistans Ambassade v. Shah Travel*, UfR 1999.939 H (Supreme Court of Denmark 5 March 1999) (Case about personal difference that was not affected by International Law on Diplomatic Immunity).

[154] On such exorbitant jurisdictional rules and international law, see SPANG-HANSSEN-2 *supra* note 3, Chapter 26 section 1.1 and 1.2 and Chapter 31 section 3.3.

[155] F.T. *supra* note 49, 1985-86, Supplement A, column 2949. Otherwise, BET 1052/85 *supra* note 42, at 19 that holds the length and purpose of the stay is without importance.

[156] *Islandsk Kompagni A/S v. Oskar Halldorsson*, UfR 1927.516 SH (The Maritime and Commercial Court in Copenhagen, 4 February 1927) (An Icelander, that temporary stayed at a hotel in Copenhagen, could pursuant to the provision be sued at The Maritime and Commercial Court in Copenhagen).

[157] Act no. 325 of 4 June 1986 on the E.U. Court-convention, article 3 of the Brussels Convention and preamble no 22 and article 3 of the E.U. Council Regulation 44/2000.

[158] That is, Iceland, Norway, Switzerland and the Member States of the E.U. See article 3 of the Brussels Convention 16 September 1988 on jurisdiction and the enforcement of judgments in civil and commercial matters and Protocols hereto.

of jurisdiction and the lawsuit concerns financial circumstances it can be brought at the court at the place where the defendant has property at the time of filing the suit or where the property that the dispute concerns is located at the time when the suit is filed.[159]

This exorbitant[160] jurisdiction provision, which is subsidiary, concerns financial circumstances, that is, plaintiff seeking a judgment for execution as well as action for a declaration with a claim, which has economic value and is bases on civil law.[161] The "Goods-jurisdiction-rule" ["Godsværnetinget'] can be used to both natural and juristic persons,[162] except against persons in E.U. Member States[163] or persons living in States covered by the Lugarno Convention. [164] Another exception for the use of the provision is bankruptcy. A foreign plaintiff pursuant to provision can sue other foreigners in Denmark at the place of the property at the time of filing the lawsuit.[165]

The plaintiff has the burden of proof as to show the foreign defendant has property in Denmark at the time of filing the lawsuit.

By "property" ["gods"] the provision in § 246 subsection 3 means principally everything of economic value,[166] in example movables, debt and rights

[159] "At the time when the suit is filed" ["Sagens anlæg"], that is the time when the plaintiff's writ/written complaint is received by the court, compare Rpl § 348 subsection 1.

[160] In Denmark, the courts are not allowed to reject cases on basis of the doctrine of forum non-convenience, see above note 139.

[161] CIVILPROCESSEN *supra* note 15, at 124 and ALLAN PHILIP *supra* note 5, at 94.

[162] KOM RPL-I *supra* note 53, at 385 note 15.

[163] Act no. 325 of 4 June 1986 on the E.U. Court-convention, article 3 of the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters and preamble no 22 and article 3 of the E.U. Council Regulation 44/2000. *Skandinavisk Salgs Service ApS v. S* (Sverige), UfR 2000.493 Ø (Easter Appeal Court 30 November 1999)(An address in the Danish town of Aarhus that a Swedish firm rejected could not be basis for the transfer of a case to the court in that town - The case covered by the Brussels Convention).

[164] That is, Iceland, Norway and Switzerland and the Member States of the E.U. See article 3 of the Lugano Convention of 16 September 1988 on jurisdiction and the enforcement of judgments in civil and commercial matters and Protocols hereto.

[165] ALLAN PHILIP *supra* note 5, at 96.

[166] *Eti-Tuber A/S v. Firma Theodor Klass* (Germany), UfR 1968.336 V (Western Appeal Court 18. December 1967) (Danish firm claimed damage caused by breach of contract

(including title) of any kind.[167] Danish patent and trademark rights allow the use of the "Goods-jurisdiction-rule" and thus allow Danish courts the exercise jurisdiction;[168] whereas it is doubtful whether other immaterial or incorporeal rights allow use of the provision.[169] The existence of a right to protection by copyright of an intellectual achievement alone does not justify the use of the "Goods-jurisdiction-rule."[170] The ordinary right to protection in Denmark of the rights of an author or artist or of unregistered marks or brands does not support jurisdiction in Denmark for an author or artist, which lives abroad. The comment to the bill holds the provision can be used where the suit concerns a claim of title or proprietary right or limited rights to propriety in Denmark, including debt.[171]

Thus, a foreigner's economic claim against a person staying in Denmark can support exercise of jurisdiction in Denmark pursuant to the "Goods-jurisdiction-rule."[172] This is also the case in a dispute between the same par-

of a German firm, who's Danish attorney had a cash deposit that a Danish court on behalf of the Danish firm had made attachment into. This deposit as "goods" could make basis for exercising jurisdiction). *Nordisk Rederiaktieselskab v. Firma Terwogt & Lagers* (Holland), UfR 1960.434 SH (The Maritime and Commercial Court in Copenhagen 29 December 1959)(Allowed exercise of jurisdiction on basis of a attached money deposit at the Danish agent of a Dutch company and which deposit was not the base of the dispute).

[167] CIVILPROCESSEN *supra* note 15, at 126 and ALLAN PHILIP *supra* note 5, at 96. *Firmaet M Friis-Møller & Co v. Firmaet Tandberg & Wigeland* (Norway), UfR 1930.402 Ø (Easter Appeal Court 31 January 1930)(A Norwegian firm that had a mortgage in Denmark had "goods" in Denmark and could be sued in Denmark in a case concerning damage (not base done the Danish Patent Act).

[168] CIVILPROCESSEN *supra* note 15, at 126-27.

[169] ALLAN PHILIP *supra* note 5, at 97.

[170] *Brunswick A.G. v. C.E. Jensen*, UfR 1964.228 H (Supreme Court of Denmark 14 February 1964) (Held the right to an architect-project about a rebuilding of a hall in Denmark was located at the place of the owner of the right) and the comment of Supreme Court Judge P. Spleth, *Retspleje i borgerlige sager - Udlændinges værneting* [Administration of justice in civil cases - Foreigners Jurisdiction], JOURNAL OF LAW PART B 1964B.264. The decision is thoroughly reported below in footnote 184.

[171] F.T. *supra* note 49, 1985-86 Supplement A, column 2949, KOM RPL-I *supra* note 53, at 389 note 19 and CIVILPROCESSEN *supra* note 15, at 128.

[172] *Handelsfirmaet Vacuum Oil Co A/S v. R Mithassel*, UfR 1921.908 SH (The Maritime and Commercial Court in Copenhagen, 26 August 1921) (Provision in Rpl. §248 sec-

ties, that is, the property is the foreigners claim (counterclaim) on the person that sue the owner of the property (the foreigner) for some (other) claim - even if the two claims arise from the same matter or contract. It is a condition that the counterclaim is independent of the plaintiffs claim, and that the plaintiff has not "created" the property by not paying the counterclaim at the time of payment.[173] Use of the "Goods-jurisdiction-rule" can be prohibited caused by a special nature of the matter in question. Setting up a counterclaim from the plaintiff that has reached the defendant before the lawsuit probably allows use of the counterclaim as basis for jurisdiction in Denmark pursuant to § 246 subsection 3 even if defendant contests the main-claim and thus the counterclaim.[174] The counterclaim must exist at the time when the suit is filed. A counterclaim is terminated if square by a set-off had been done before filing the suit,[175] however, it might be by analogy with the decision in UfR 1944.682 SH [176] that defendant cannot by setting off a small counterclaim with a part of a larger main-dept can eliminate the possibility of testing the

tion 2 allowed used on basis of a debt on a foreigner transported from a foreign firm to its Danish sister company).

[173] *Johann H. Anthon A/S v. Bogesundsmaskiner AB* (Sverige), UfR 1971.512 V (Western Appeal Court 3 February 1971) (A Danish distributor to a Swedish firm could not avoid paying its overdue dept for delivered spare part to the distributor in an attempt to create jurisdiction in Denmark for a commission that the Danish distributor claimed to have against the Swedish firm. At least the main part of the Swedish firm's claim was overdue when the dispute arose), CIVILPROCESSEN *supra* note 15, at 128-129 and ALLAN PHILIP *supra* note 5, at 99. Compare *Allan Haugsted v. Firma Maretec A.G*. (Switzerland), UfR 1990.475 V (Western Appeal Court 1 March 1990) (As a Danish plaintiff had neither fully nor partly acknowledged a counterclaim from a Swiss company, the counterclaim could not be "goods" in the sense of §246 subsection 3).

[174] CIVILPROCESSEN *supra* note 15, at 129.

[175] See below footnote note 173.

[176] UfR 1944.682 SH (The Maritime and Commercial Court in Copenhagen, 4 February 1944) (A Danish charterer B of a Finish vessel, which had a dispute with a shipping owner R about demurrage, deposited the amount of 2,500 in Danish currency at a brokerage house. B acknowledged a debt of 195 in Danish currency and tried to use this as basis for jurisdiction pursuant to Rpl. §248 subsection 2 in a case against R with claim of release of the rest of the deposit. Case dismissed as the 195 DKK could not be accepted as a separate "goods", but had to be regarded as part of the deposit that could not be regarded as "goods" belonging to R).

validity in court of the remaining part of the main-claim, if defendant at the same time rejects the validity of the main-claim.

Contrary to previous times, [177] claims that are denied can now be basis for use of the "Goods-jurisdiction-rule."[178]

It is a requirement that the property (effects) can be located in Denmark at

[177] H. Munch Petersen in JOURNAL OF LAW PART B 1926B.45 ff and BET 1052/85 *supra* note 42, at 81. ALLAN PHILIP *supra* note 5, at 99, remarks that Danish professor Erik Siesby has criticized case law in *Godsværnetinget og forum rei sitæ* [The goods-jurisdiction rule and forum rei sitæ], JURISTEN 1974.84 and Erik Siesby, *Udlændinges værneting og udlandsdanskeres* [Foreigners jurisdiction and Danes abroad], JOURNAL OF LAW PART B 1980B.381. *A/S Svendborg Kasein v. Freddy Baines S.A*., UfR 1956.657 H (Supreme Court of Denmark, 7 May 1956) (Held consignment from outside Denmark was partly in conflicting with a contract. Application for arrest of property dismissed as the foreigner did not have any "goods" in Denmark, because the dispute was about the ownership of the consignment itself) and the decision in *A/S Svendborg Kasein v. Freddy Baines S.A*., UfR 1955.1079 SH (The Maritime and Commercial Court in Copenhagen 8 July 1955) (Service of process to the President of a foreign corporation under a stay in Denmark could not allow exercise of jurisdiction over the foreign corporation)). Danish Professor Allan Philip criticize the decision in *Nordisk Fjer A/S v. Firma Samuel Motzen* (Romania) UfR 1942.660 SH (The Maritime and Commercial Court in Copenhagen, 27 March 1942), where the purchase price for the redemption of the documents of a consignment could not be the basis for the "Goods-jurisdiction-rule" in a case concerning damage caused by defects in the purchased goods. *Firmaet Harald Kjær & Co v. Rederiet Nielsen & Thorden O/Y* (Helsinki, Finland), *Forsikrings-Aktieselskabet Urania v. "Madrid, Sociedad anonima de reaguros"* (Spain), UfR 1926.84 H (Supreme Court of Denmark 22 December 1925) (Insurance company, which owed a Spanish insurance company an amount in Spanish currency, could not use the debt as basis for creating jurisdiction in Denmark in a case concerning making up other of their outstanding economic difference.

[178] The possibility of denial of jurisdiction bases on "goods" in cases where the existence of "goods" depend on the result of the case are not available in all States, compare CIVILPROCESSEN *supra* note 15, at 128 note 99 and Erik Siesby, *Udlændinges værneting og udlandsdanskeres* [Foreigners jurisdiction and Danes abroad], JOURNAL OF LAW PART B 1980B.378. *Kilchem Adriatic of 25/6/1993 A/S v. Office National de l'Huile* (Tunisia), UfR 1996.950 SH (The Maritime and Commercial Court in Copenhagen 22. April 1996)(A claim that was put forward by defendant at a court in Tunisia against a Danish company, which denied the claim, could be basis for the "Goods-jurisdiction-rule" and thus allow a lawsuit in Denmark against the Tunisian company).

the time of filing the lawsuit.[179] In this respect is must as for the use of §246

[179] BET 1052/85 *supra* note 42, at 20. **From Danish case law:** *Capstan Shipping Ltd. ApS v. ScanPly International Wood Products Ltd*. (Hong Kong), UfR 1988.579 SH (The Maritime and Commercial Court in Copenhagen, 24 February 1988) (Bank accounts in Denmark, which a foreign company to a certain degree itself could make arrangements about, allowed jurisdiction in Denmark in a case against the company), *Shen-Har Investment & Development Ltd*. (Israel) *v. Fa. Edelstein Pfanzen* (Germany), UfR 1988.426 Ø (Easter Appeal Court 14 December 1987) (S in Israel sold goods to K1 in Germany, which resold to K2 in Denmark and transferred S its claim on K2. A dispute about faults in the goods arose between S and K1, where after K2 deposited the payment in a Danish bank. The deposited amount allowed S the use of the "Goods-jurisdiction-rule" against K1), *Bauherrengemeinschaft* (Germany) *v. Konkursboet Bent Iversen*, UfR 1987.14 H (Supreme Court of Denmark 13 November 1986)(Appellant's claim of dismissal of one of a bankrupt estate filed lawsuit rejected, since the appellant, which had made no claim in the bankrupt estate, against the bankruptcy estate had either the right to the deposited amount that the lawsuit was about or a claim that was not without value), *Industriaktiebolaget EUROC v. Inger Topsøe & Swegon AB* (Sweden), UfR 1987.690 H (Supreme Court of Denmark 15 July 1987)(The "Goods-jurisdiction-rule" based on a claim that had been filed as proof against a bankrupt estate, since the claim was not without any value, even though creditor had given his consent so the claim became was placed at the end in the bankruptcy estate), *S. Bjerregaard & Sønner Fiskeeksport A/S under konkurs v. Gulf Fish Trading Ltd.* (Holland), UfR 1999.88 H (Supreme Court of Denmark 19. October 1998)(Dutch company's unchallenged claim of 10.177 in Danish currency against a bankruptcy estate could be basis for a lawsuit pursuant to § 246 subsection 3, even though the claim had not, but could file a proof of a claim against a bankrupt estate), *Triplex S.p.A.* (Italy) *v. Haka-Kirk Husholdningsmaskiner A/S under konkurs*, UfR 1972.714 H (Supreme Court of Denmark 6 June 1972)(A bankruptcy estate was allowed in Denmark suing an Italian company, as the latter, which had filed a proof of a claim against the bankrupt estate, was held to have "goods" in Denmark, even though dividend would not extent the amount of the claim in the lawsuit. A draft from the accountant of the bankruptcy estate suggested a dividend of 12 percent. It was held that it could not be disregarded that "some" dividend might be paid out), *Firma Electronic v. Konkursboet Stenløse Plastic*, UfR 1978.876 H (Supreme Court of Denmark, 2 October 1978)(Claim filed as proof against a bankrupt estate was "not without value"), *Niels Mousten Vestergaard v. European Homes B.V. & European Construction B.V*. (Netherlands), UfR 1977.395 Ø (Easter Appeal Court 22 December 1977)(In a lawsuit against a Danish registered limited partnership third party notice was given to two foreign corporations, which owned the whole subscribed capital of the Danish limited partnership, who's funds pursuant to the two foreign corporations all had been expended whereby there was no means to

subsection 3 be determined when a right (including title) or a debt is located in Denmark, even if it is a fiction to talk of a "location" of a right and claim.[180] It is presumed that an ordinary debt in relation to §246 subsection 3 is located in Denmark, if the debtor has residence in Denmark.[181] If the claim arises from a negotiable document, the venue is at the place where the document is.[182]

Danish professor Allan Philip holds the future possibility of execution of the property is an essential element in the rational explanation of existence of

cover the costs of a liquidation. Held there was "goods" in Denmark allowing the lawsuits against the two foreign corporations, since the limited partnership original was made up with a subscribed capital of 100.000 in Danish currency with purpose of doing business in Denmark, that the foreign corporations owned the whole subscribed capital, and that these two corporations had not decided to initiate a winding-up). Opposite: *Aage Thorning-Christensen v. Ella Hartvig Henriksen*, UfR 1945.393 Ø (Easter Appeal Court, 19 December 1944) (Foreigner had mortgage deeds with security in real estate in Denmark. No "goods" pursuant to the "Goods-jurisdiction-rule" as the deed-documents was physical outside Denmark), *Bent Bjerregaard Thomsens konkursbo v. Astramaris Schifahrtskontor G.m.b.H.* (Germany), UfR 1973.206 V ((Western Appeal Court, 13 November 1972)(Neither the debt-claim against bankruptcy estate, who's means was expected only partly to cover preferential claims, or the personal claim against the bankrupt person, could be regarded as "goods" and support jurisdiction), *H.H.Andersen Konfektion Aps v. Textilwerke Ganahl A.G*. (Austria), UfR 1997.565 SH (The Maritime and Commercial Court in Copenhagen, 24 March 1977)(The "Goods-jurisdiction-rule" not used as a foreigner's claim based on a bill of exchange against a Danish plaintiff was not regarded as "goods" pursuant to Rpl. §248 (now §246) subsection 2).

[180] ALLAN PHILIP *supra* note 5, at 96.

[181] ALLAN PHILIP *supra* note 5, at 97, Statement no. 103 of 13 September 1921 from Law Council [Retsrådet], JOURNAL OF LAW PART B 1921B.344 (The term "goods" ["gods"] also covers claims. Thus a lawsuit can be filed in Denmark if the claim is based on a borrower's note and this note is in Denmark, or a claim made oral by a person that lives in Denmark), Supreme Court Judge P. Spleth: *Retspleje i borgerlige sager - Udlændinges værneting* [Administration of justice in civil cases - Foreigners Jurisdiction], JOURNAL OF LAW PART B 1964B.264 and Jens Anker Andersen in *Kreditorforfølgning mod kontantindeståender i pengeinstitutter* [Execution into cash deposits in financial institution], JURISTEN 1972.433, 453.

[182] CIVILPROCESSEN *supra* note 15, at 126 and ALLAN PHILIP *supra* note 5, at 97.

the "Goods-jurisdiction-rule."[183] It is presumed that use of §246 subsection 3 is not barred in instances where execution in the property pursuant to other rules are prohibited, or where the effects are embraced by the guarding rule in Rpl. §509 ("trangsbeneficiet"), or where the property is in a trust fund.[184] The property must have a certain clarity and certitude. Credit facility, for example drawing right to an overdraft facility, cannot be "property" in harmony with Rpl. § 246 subsection 3.[185]

As "property" is regarded, property the foreign defendant possesses or legally has at his disposal at the time of filing the suit.[186] Further, claims targeting property in Denmark, that a foreigner argue is his, but which he does not possess, should allow use of the "Goods-jurisdiction-rule."[187] If the property is transferred to a third party before the time of the filing of the lawsuit, the provision does not allow exercise of jurisdiction pursuant to § 246 subsection 3.[188] The fact that defendant in case of a judgment requiring him to pay the

[183] Likewise Danish professor Erik Siesby, *Godsværnetinget og forum rei sitæ* [The goods-jurisdiction rule and forum rei sitæ], JURISTEN 1974.84, 85. Danish professor Allan Philip notes, that case law, except from the *Handelsfirmaet Vacuum Oil Co A/S v. R Mithassel,* UfR 1921.908 SH (see above footnote 172), all made debtors residence in Denmark be determining of whether enforcement of debts could be granted, ALLAN PHILIP *supra* note 5, at 97 and Mogens Munch, *Udlæg i fordringer på en skyldner i udlandet* [Execution into debt of a person outside Denmark], JOURNAL OF LAW PART B 1966B.217, 226. *Københavns ny Tømmer-Handel A/S v. Rederiet for m/s "Alma"*, UfR 1951.1117 SH (The Maritime and Commercial Court in Copenhagen 27 April 1951) (Arrest of property for a compensation claim was done into an amount of freight. The latter could not be base for jurisdiction about another claim as the seizure amount was presumed to fully cover the first made claim).

[184] CIVILPROCESSEN *supra* note 15, at 127.

[185] KOM RPL-I *supra* note 53, at 387 note 18.

[186] *Shirley Jean Nielsen* (Nevada, USA) *v. Margot Engsig-Karup* (Denmark), UfR 1977.887 V (Western Appeal Court 22 July 1977) (Lawsuit in Denmark against a person now residence in the U.S. dismissed as one of the plaintiff issued purchase-money mortgage was sold by the sued person before the time of filing the lawsuit in court).

[187] Erik Siesby, *Godsværnetinget og forum rei sitæ* [The goods-jurisdiction rule and forum rei sitæ], JURISTEN 1974.84, ALLAN PHILIP *supra* note 5, at 97 and KOM RPL-I *supra* note 53, at 363.

[188] If a foreign seller has obtained advance payment in his bank against security in documents of the bargain, the seller's claim against the debtor cannot be used as "goods" pursuant to §246 subsection 3 if the security has such an extent that there will be no

main-claim has the possibility of later setting-off cannot hinder use of the "Goods-jurisdiction-rule" on basis of the counterclaim, since it is the situation at the time of the filing of the suit that is the decisive pursuant to § 246 subsection 3.[189] The plaintiff must not base the existence of the property in Denmark on unilateral or unfair transaction.[190]

The property must have such a value that the foreigner altogether has consideration as to in future using his rights as owner.[191] Danish professor Allan Philip holds[192] the decision in *Inter System Transport Ltd. (England) v. Hans*

surplus for the seller. Jens Anker Andersen, *Kreditorforfølgning mod kontantindeståender i pengeinstitutter* [Execution into cash deposits in financial institution], JURISTEN 1972.433, 454 & *A/S Frederik Fiedler v. Firmaet E. Zoubir* (Algeria), UfR 1925.453 SH (The Maritime and Commercial Court in Copenhagen, 31 March 1925)(A buyer wanted to make arrest into the amount he had paid to the Danish bank Privatbanken, which had received an invoice as basis for debt collecting from a bank in Algeria concerning another claim against the seller in Algeria. The paid amount belonged to the bank in Algeria and thus could not be "goods"), *A/S Jølving v. firmaet Wallengreen & Co* (Sweden), UfR 1954.609 SH (The Maritime and Commercial Court in Copenhagen, 12 March 1954)(Transfer of a claim to avoid it could be used as basis for the "Goods-jurisdiction-rule" allowed), *Bjørn Bartig* (Sweden) *v. Den Danske Landmandsbank A/S*, UfR 1968.384 H (Supreme Court of Denmark, 1 April 1968)(Transfer of rights not allowed and therefore "goods" existed in Denmark).

[189] ALLAN PHILIP *supra* note 5, at 100.

[190] CIVILPROCESSEN *supra* note 15, at 129, Erik Siesby, *Udlændinges værneting og udlandsdanskeres* [Foreigners jurisdiction and Danes abroad], JOURNAL OF LAW PART B 1980B.378, 380. *A Munck v. Alkan, Heumann & Co*. (Germany), UfR 1924.350 SH (The Maritime and Commercial Court in Copenhagen, 13 February 1924)(The "Goods-jurisdiction-rule" did not allow a buyer staying in Denmark the right to sue the foreign seller for a compensation claim, since he abstained from paying the purchase price of a consignment), *Ole Bruun ApS v. Schmict O.H.G. Lederfabrik und Kunststoffwerke* (Austria), UfR 1978.863 Ø (Easter Appeal Court, 19 June 1978)(As the claim that should be the base for jurisdiction arose from the debtors negligence of payment of delivered goods, the foreign creditor's claim could not be regarded as "goods" in a case concerning the debtor's compensation claim against the creditor).

[191] CIVILPROCESSEN *supra* note 15, at 125-127 and ALLAN PHILIP *supra* note 5, at 96 and Supreme Court Judge P. Spleth, *Retspleje i borgerlige sager - Udlændinges værneting* [Administration of justice in civil cases - Foreigners Jurisdiction], JOURNAL OF LAW PART B 1964B.263-265.

[192] ALLAN PHILIP *supra* note 5, at 96.

Erik Harbos konkursbo[193] might suggest that the relationship between the claim and the property in Denmark can be influence what will be asked for as to the value of the property. On the other hand will a totally worthless effect or a property that defendant prior to the lawsuit has given up or thrown away, or that the foreigner caused by its value must be presumed not will make efforts to regain, not support jurisdiction pursuant to the "Goods-jurisdiction-rule."[194] Some kind of a lower limit must be expected.[195]

If the above mentioned is related to computer network where the potential defendant is a non-E.U. foreigner, electronic money[196] over which bookkeeping is done in Denmark must be regarded as "property" in the sense of § 246 subsection 3, similar to deposits in Danish financial institution in which case

[193] *Inter System Transport Ltd.* (England) *v. Hans Erik Harbos konkursbo*, UfR 1974.548 H (Supreme Court of Denmark, 28 May 1974) (English company had one of a bankruptcy estate recognized claim of 15.238,50 in Danish currency. The expected dividend was 1.77 percent, or 269.72 in Danish currency. This could be basis for jurisdiction pursuant to the "Goods-jurisdiction-rule" in a case concerning invalidation of another difference).

[194] Supreme Court Judge P. Spleth, *Retspleje i borgerlige sager - Udlændinges værneting* [Administration of justice in civil cases - Foreigners Jurisdiction] in JOURNAL OF LAW PART B 1964B.263, 265 containing comments to the decision in *Brunswick A.G. v. C.E. Jensen*, UfR 1964.228 H (Supreme Court of Denmark, 14 February 1964) (Some board partitions had been set up in a hall in Denmark by a foreign company with the purpose to make a bowling alley, which project was later abandoned. After removal of the partitions and re-establishment of the previous condition of the hall, the board partitions would have a net value of 140 in Danish currency. The plaintiff claimed the project of the architect (whose fee was 30.000 in Danish currency) and the board partitions should be regarded as "goods" pursuant to the "Goods-jurisdictional-rule". As for the project of the architect the Supreme Court of Denmark held the architectural drawing could not be "goods" and find it determining where the "project" as a right physical was. The right had to be at the place of the rights holder, that is, the legal person that in the case in question was in Switzerland. As for the board partitions the Supreme Court of Denmark held these could not in a case against the foreign company be regarded as "goods" as they did not have such a value that any of the parties would take it into consideration unless for the issue of achieving jurisdiction in Denmark).

[195] CIVILPROCESSEN *supra* note 15, at 125-127.

[196] Means of payment, which are stored on electronic media, and recognized as monies by other firms that the issuer, BRYDE ANDERSEN *supra* note 33, at 802, section 20.4.g.

it has not influence where the customer or the passbook is located.[197]

On the other hand, a foreigner will probably not have "property" in Denmark if the foreigner is owner of a domain name under ".dk", which is issued by the Danish company DK-Hostmaster with a certificate, and the certificate is kept outside Denmark.[198]

In general should a foreigner's website, that is stored on a server in Denmark, not be regarded as "property" in the meaning of § 246 subsection 3 as it can be the foreigners web administrator that owns the rights to the site, just as well as there in practice will be a significant problem achieving evidence of whether the website is placed by the foreigner defendant himself, or it only is a copy-website placed (automatically) by the network of efficiency reasons or by the foreigner's server host.

The fact that a foreign artist as his only media for publication uses a website placed in Denmark and on this website uploads his work in form of music-files or (book) text-files from which site other persons can read, listen or download the files, will probably not be "property" in the meaning of the "Goods-jurisdiction-rule", compare with the decision in *Brunswick A.G. v. C.E. Jensen*,[199] because the foreigner as the copyright owner is located outside Denmark and most probably has a copy of the files ("the right") at his own place.

9.3. Enforcement/Execution

Pursuant to public international law States have no obligation to recognize foreign court judgments[200] and thus international competence of courts, unless the State of the court in question has made a treaty on recognition and enforcement of judgments from courts of the other party.[201] It should be pointed out, that in public international law it is quite different rules that regu-

[197] See above UfR 1968.336 V and UfR 1960.434 SH in footnote 166 and UfR 1988.579 SH in footnote 179.
[198] See above UfR 1945.393 Ø in footnote 179 and UfR 1977.887 V in footnote 186.
[199] UfR 1964.228 H mentioned in footnote 194.
[200] SPANG-HANSSEN-2 *supra* note 3, Chapters 28 and 33.
[201] ALLAN PHILIP *supra* note 5, at 81-82.

late legislative jurisdiction respectively enforcement.[202]

Professor F.A. Mann has stated that it is probably the question of enforcement and not legislative jurisdiction, which has the most vital interest of States.[203] The progress over the last ten years of the Hague Conference on a draft convention on jurisdiction, recognition and enforcement show how difficult it is to unite the different point of view into one regime and thus recognize foreign countries rules of jurisdiction and judgments.[204]

This schism seriously influence on the citizens in the different States, because as citizens cannot get judgments achieved in their own State courts executed in the foreign State where the defendant stays, the achieved judgments is in reality of none value for the citizen (plaintiff) that have become somewhat without legal rights in the international community.

Commentary to the Civil Procedure Code[205] remarks that the range of the special consumer-jurisdiction-rule in Rpl. § 246 section 1, 2 sentence probably is limited as it is very likely a Danish court decision achieved by a Danish consumer against a foreigner staying outside the territories of the E.U. and the Nordic countries will not be recognized and/or enforced in the State where businessman lives

In Denmark, a request for enforcement of a court decision shall be filled a bailiff's court.[206] A Danish bailiff's court can levy execution on judgment debtor's property if distrainee has residence in Denmark or in lack of residence at the place in Denmark where he is found or has property.[207] Seizure cannot be done into objects that are placed outside Denmark. As for foreign bank deposit, execution can be done if a passbook as an identification papers has been issued and is placed in Denmark. In other circumstances, execution

[202] MANN-1 *supra* note 20, at 128.

[203] MANN-2 *supra* note 21, at 18.

[204] A short report of the progress is given in SPANG-HANSSEN-2 *supra* note 3, at 453-458.

[205] KOMMENTERET RETSPLEJELOV [Commentary to the Civil Procedure Code] Vol. -II page 385 note 7 (6. Ed. 2000).

[206] Civil Procedure Code Chapter 46 (§487).

[207] *K v. Fogedretten i X-by,* UfR 2003.136 V (Western Appeal Court 7 March 2003) (Execution by a bailiff on basis of a judgment over a Dane now resident in Greenland [Greenland has its own Civil Procedure Code] had to be carried out at the place of debtor's "home jurisdiction" and not at the place where debtor had assets (real estate in Danish town X)).

is presumed out of the question, since a Danish act of execution cannot be expected to be recognized in a foreign State.[208] In Danish legal usage has been incidents where execution has been done into ordinary debt of foreign debtors, see *Købmand Bernhard Petersen* (Iceland) v. *Købmand P.J. Torfason* (Iceland)[209] and *Direktoratet for Københavns skattevæsen v. Poul Ingvar Steen*,[210] however, this practice is hardly valid.[211]

The Minister of Justice is pursuant to Rpl. § 479 legitimated to issue provisions that allow decisions of civil matters from courts or executives of foreign States to be executes in Denmark on the condition that the decision can be enforced in the original State or the State who's law is basis for the decision, and execution will not be obvious inconsistent with the States legal system.[212] The Danish Minister of Justice has yet not used the authorization.

[208] Jens Anker Andersen, *Kreditforfølgning mod kontantindeståender i pengeinstitutter* [Execution into cash deposits in financial institution], JURISTEN 1972.433.

[209] *Købmand Bernhard Petersen* (Iceland) v. *Købmand P.J. Torfason* (Iceland), UfR 1920.626 Ø (Easter Appeal Court, 10 May 1920)(Icelander D had a claim (circa 10.000 in Danish currency) on another Icelander H, which claim K made arrest of property into by the bailiff of Copenhagen while D temporary stayed in Denmark. The arrest was upheld by a judgment a time after D had returned to his residence on Iceland, where he stayed at the time of executing the enforcement of the judgment. K notified H by registered mail about the arrest and its legal consequences. D argued that execution could not be done, because he only had stayed temporary in Denmark, that the claim was not recognized by any written document, and that either creditor or debtor resided or stayed in Denmark at the time of execution done by the bailiff. The Appeal Court held that at least under the particular given facts in that case execution could be done into the seizured property (debt), even though creditor and debtor did not live or stayed in Denmark at the time of the enforcement of the judgment).

[210] *Direktoratet for Københavns skattevæsen v. Poul Ingvar Steen*, UfR 1964.224 H (Supreme Court of Denmark, 10 February 1964) (Attempt of execution in Denmark into cash in an American bank belonging to an American citizen without having a court decision from an American court).

[211] Jens Anker Andersen, *Kreditforfølgning mod kontantindeståender i pengeinstitutter* [Execution into cash deposits in financial institution], JURISTEN 1972.433, 444.

[212] PAUL KRÜGER ANDERSEN M.FL., DANSK PRIVATRET 31 (12. Ed., DJØF Publishing 2001).

9.4. Final Remarks

It might help Danish consumers if they from the Danish jurisdictional rules could read to what extent they were truly protected in stead of existing theoretical and political influenced consumer protection provisions that gives the consumer the illusion of being protected through Danish court decisions that the consumer afterwards realize cannot be enforced against the foreign party.

If professor Lawrence Lessig[213] and several others are right that "code is law", and if the TCP/IP-protocol according to the constructors of Internet is the "Constitution of the Internet", and none of the users of the World (governments, international organizations and individuals) since establishment of the protocols has demanded it changed, one could fairly assert, that this international basic protocol-code for international computer network, which Lessig describe as law, has become customary international law,[214] which can be advanced before the International Court of Justice in the Hague.

This imply that if a Danish jurisdiction rule related to foreigners, which have used international computer networks, is in inconsistent with the principal principles of the TCP/IP protocol (for example free speech and exchange of information on the Net) the Danish rule is null and void. The problem is that Danish courts have no competence to refuse such lawsuits.

As it is impossible to anticipate, which new techniques that will be developed on the computer networks - and with the extreme pace the technology changes - it seem imperative and urgent that Danish judges - at least in relation to cases involving foreigner dealings on international computer networks - by the legislators are given the possibility of discretionary decide to reject lawsuits in cases where the court finds there is not sufficient closeness and

[213] Lawrence Lessig, *Legal Issues in Cyberspace: Hazards on the Information Superhighway: Reading the Constitution in Cyberspace*, 45 EMORY.L.J. 869, 899 (1996) and LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999 - ISBN 0-465-03913-8).

[214] Pursuant to STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW as amended at the 2000 London conference (International Law Association) nr. 11 page 19 customary law can be created by international organizations. The organs behind the TCP/IP-protocol can fairly be recognized as such international organizations, <http//:www.ila-hq/pdf/CustomaryLaw.pdf>.

link to Denmark or that it would not be reasonable to hear the case.

It should not be forgotten that if the TCP/IP protocol shall have the ability to work equal and fair to everybody one has, when the issue is "pure" online bits-transmission, to work with rules that express all or the intersection of the greatest possible number of countries - not a union of rules - that is, local peculiarity and characteristic has to be shut out.

If Denmark wants to be a IT-pioneer-country – as the present Danish Government wants - it should introduce a special international jurisdiction on computer network, that allow jurisdiction in Denmark in cases involving business websites (outside the E.U. territory)[215] that are especially targeting Denmark and through which site profit from Denmark has been gained in more than few or fortuitous incidences. Further, such rule should also allow jurisdiction in case of a wrong when the content of the website has pinpointed to persons in Denmark, but in cases where referring to a larger group of persons that might feel hurt or indignated by the content on the website. Furthermore, such a special provision should provide the judge a discretionary obligation to hold based on the facts of the case that it is reasonable from the foreign defendant's point of view to hear the case, including a determination of whether the plaintiff in reality has been the strong part (for example by use of a electronic agent or Bot), and whether the foreigners dealing is legal in his own State.

Finally, where the content of a foreign website (outside the E.U. territory) contain user-terms that the foreigner can prove a Danes' electronic agent has accepted, the Dane should be bound of these terms, for example choice of jurisdiction and choice of law. This should perhaps also be the case where a Dane buys effects from foreign auction sites and where the seller is a consumer.

[215] In this connection should not be forgotten that Scandinavian users seem to prefer foreign websites to those of Danish (Scandinavian) versions and thus chooses to "go abroad", which fact has resulted in American Yahoo! to shut down its Danish (and other Nordic) website-versions, see above footnote 8.

APPENDIX

1. U.S. States with statutes on basis of the Single Publication Model Act

- Arizona effective July 1st 1953 as A.R.S. § 12-651.
- California effective September 7th 1955 as West's Ann.Cal.Civ.Code §§ 3425.1 - 5.
- Florida, Fla. Stat. §770.06 (1967)
- Idaho effective March 7th 1953 as I.C. §§ 6-702 - 705.
- Illinois effective July 22nd 1959 as S.H.A. ch. 126, §§ 11 – 15
- Nebraska, Neb. Rev. Stat §20-209 (1983)
- New Mexico effective March 3rd 1955 as NMSA 1978, §§ 41-7-1 - 5.
- North Dakota effective March 13th 1953 as NDCC 14-02 - 10.
- Pennsylvania effective August 21st 1953 as 42 Pa.C.S.A. §8341

2. U.S. States that have adopted the Single Publication Rule by case law

- Alabama – Proctor v. Gissendaner, 579 F.2d 876 note 7 (5th Cir. 1978), Age-Herald Publishing Co. v. Waterman, 188 Ala. 272 (Ala., 1921)
- Alaska – McCutcheon v. State, 746 P.2d 461
- Colorado – Living Will Center v. NBC Subsidiary Inc., 857 P.2d 514 (Colo.App. 1993)
- Connecticut – Dale System v Time. Inc., 116 F.Supp. 527 (D.Conn. 1953)
- District of Columbia - Ogden v. Association of the Untied States Army, 177 F.supp. 498 (D.C.C. 1959)
- Georgia - Carroll City/County Hosp. Auth. v. Cox Enterprises, Inc., 147 GA.App. 863 (Ga.App. 1978)
- Kansas - Fouts v. Frawcett Publications, 116 F.Supp. 535 (D.Conn. 1953)
- Louisiana – Brian v. Harper, 144 La. 585 (La. 1919)
- Maryland – Hickey v. St. Martin's Press, Inc., 978 F.Supp. 230, 236 (D.Md. 1997)
- Massachusetts - McGlue v. Weekly Publications, 63 F.Supp. 744 (D.Mass. 1946)
- Michigan - Tocco v. Time, Inc. 195 F.Supp. 410(E.D.Mich. 1961)
- Minnesota - Church of Scientology of Minnesota v. Minnesota State Medical Ass'n Fdn., 264 N.W.2d 152 (Minn. 1978)
- Missouri - Julian v. Kansas City Star Co, 209 Mo. 35 (Mo. 1907)
- Mississippi – Forman v. Miss. Publishers Corp., 14 So.2d 344, 347 (Miss. 1943)
- Nevada – Flowers v. Carvill, 112 F.Supp.2d 1202, 1210 (D.Nev. 2000)
- New Hampshire – Keeton v. Hustler Magazine, Inc. 131 M.H. 6 (N.H. 1988)
- New Jersey – Barres v. Holt, Rinehart & Winston, Inc., 74 N.J. 461 (N.J. 1977)
- New York - Gregoire v. G.P. Putnam's Sons, 298 N.Y. 119 (N.Y. 1948)
- Ohio, Snell v. Drew, 1985 WL 8216, 1985 Ohio App.LEXIS 9187 (Ohio Ct.App. 1985)
- Oklahoma - Hazlitt v. Fawcett Publications, 116 F.Supp 538

(D.Conn. 1953)

- Tennessee, Applewhite v. Memphis State Univ., 495 S.W.2d 190, 193 (Tenn. 1973)
- Texas - Stephenson v. Triangle Publications, 104 F.Supp. 215 (S.D.Tex. 1952)
- Vermont - Gordon v. Journal Pub. Co, 81 Vt. 237 (Vt. 1908)
- Virgina - Myska v RMS Technologies, Inc., 25 Va. Cir. 344, 1991 WL 835248, 1991 Va.Cir. LEXIS 292 (Va. Cir. Ct., 1991)
- Washington, Herron v. King Broadcasting Company, 109 Wash.2d 514, 521, 746 P.2d 295, 14 Media L. Rep. 2017 (Wash. 1987).

3. California Single Publication Rule

California Civ. Code § 3425[1]

§ 3425.1. [Citation]
This title may be cited as the Uniform Single Publication Act.

§ 3425.2. [Interpretation]
This act shall be so interpreted as to effectuate its purpose to make uniform the law of those states or jurisdictions which enact it.

§ 3425.3 [One cause of action; recovery]
No person shall have more than one cause of action for damages for libel or slander or invasion of privacy or any other tort founded upon any single publication or exhibition or utterance, such as any one issue of a newspaper or book or magazine or any one presentation to an audience or any one broadcast over radio or television or any one exhibition of a motion picture. Recovery in any action shall include all damages for any such tort suffered by the plaintiff in all jurisdictions.

§ 3425.4. [Judgment as bar]
A judgment in any jurisdiction for or against the plaintiff upon the substantive merits of any action for damages founded upon a single publication or exhibition or utterance as described in Section 3425.3 shall bar any other action for damages by the same plaintiff against the same defendant founded upon the same publication or exhibition or utterance.

§ 3425.5. [Existing causes of action]
This title shall not be retroactive as to causes of action existing on its effective date.

[1] The full text of the Uniform Single Publication Model Act is printed in section 5.5.1.2.

4. U.S. Uniform Correction or Clarification of Defamation Act ["Retraction Code"]

The U.S. Model Act of 1993 from The National Conference of Commissioners on Uniform State Laws (NCCUSL) <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/uccda93.htm> (visited March 2006):

Section 1.
Definitions.

In this [Act]:

(1) "Defamatory" means tending to harm reputation.
(2) "Economic loss" means special, pecuniary loss caused by a false and defamatory publication.
(3) "Person" means an individual, corporation, business trust, estate, trust, partnership, association, joint venture, or other legal or commercial entity. The term does not include a government or governmental subdivision, agency, or instrumentality.

Section 2.
Scope.

(a) This [Act] applies to any [claim for relief], however characterized, for damages arising out of harm to personal reputation caused by the false content of a publication that is published on or after the effective date of this [Act].

(b) This [Act] applies to all publications, including writings, broadcasts, oral communications, electronic transmissions, or other forms of transmitting information.

Section 3.
Request for Correction or Clarification.

(a) A person may maintain an action for defamation only if:

(1) the person has made a timely and adequate request for correction or clarification from the defendant; or
(2) the defendant has made a correction or clarification.

(b) A request for correction or clarification is timely if made within the period of limitation for commencement of an action for defamation. However, a person who, within 90 days after knowledge of the publication, fails to make a good-faith attempt to request a correction or clarification may recover only provable economic loss.

(c) A request for correction or clarification is adequate if it:

(1) is made in writing and reasonably identifies the person making the request;
(2) specifies with particularity the statement alleged to be false and defamatory and, to the extent known, the time and place of publication;
(3) alleges the defamatory meaning of the statement;

(4) specifies the circumstances giving rise to any defamatory meaning of the statement which arises from other than the express language of the publication; and
(5) states that the alleged defamatory meaning of the statement is false.

(d) In the absence of a previous adequate request, service of a [summons and complaint] stating a [claim for relief] for defamation and containing the information required in subsection (c) constitutes an adequate request for correction or clarification.

(e) The period of limitation for commencement of a defamation action is tolled during the period allowed in Section 6(a) for responding to a request for correction or clarification.

Section 4.
Disclosure of Evidence of Falsity.

(a) A person who has been requested to make a correction or clarification may ask the requester to disclose reasonably available information material to the falsity of the allegedly defamatory statement.

(b) If a correction or clarification is not made, a person who unreasonably fails to disclose the information after a request to do so may recover only provable economic loss.

(c) A correction or clarification is timely if published within 25 days after receipt of information disclosed pursuant to subsection (a) or 45 days after receipt of a request for correction or clarification, whichever is later.

Section 5.
Effect of Correction or Clarification.

If a timely and sufficient correction or clarification is made, a person may recover only provable economic loss, as mitigated by the correction or clarification.

Section 6.
Timely and Sufficient Correction or Clarification.

(a) A correction or clarification is timely if it is published before, or within 45 days after, receipt of a request for correction or clarification, unless the period is extended under Section 4(c).

(b) A correction or clarification is sufficient if it:

(1) is published with a prominence and in a manner and medium reasonably likely to reach substantially the same audience as the publication complained of;
(2) refers to the statement being corrected or clarified and:

(i) corrects the statement;
(ii) in the case of defamatory meaning arising from other than the express language of the publication, disclaims an intent to communicate that meaning or to assert its truth; or

(iii) in the case of a statement attributed to another person, identifies the person and disclaims an intent to assert the truth of the statement; and

(3) is communicated to the person who has made a request for correction or clarification.

(c) A correction or clarification is published in a medium reasonably likely to reach substantially the same audience as the publication complained of if it is published in a later issue, edition, or broadcast of the original publication.

(d) If a later issue, edition, or broadcast of the original publication will not be published within the time limits established for a timely correction or clarification, a correction or clarification is published in a manner and medium reasonably likely to reach substantially the same audience as the publication complained of if:

(1) it is timely published in a reasonably prominent manner:

(i) in another medium likely to reach an audience reasonably equivalent to the original publication; or
(ii) if the parties cannot agree on another medium, in the newspaper with the largest general circulation in the region in which the original publication was distributed;

(2) reasonable steps are taken to correct undistributed copies of the original publication, if any; and

(3) it is published in the next practicable issue, edition, or broadcast, if any, of the original publication.

(e) A correction or clarification is timely and sufficient if the parties agree in writing that it is timely and sufficient.

Section 7.
Challenges to Correction or Clarification or to Request for Correction or Clarification.

(a) If a defendant in an action governed by this [Act] intends to rely on a timely and sufficient correction or clarification, the defendant's intention to do so, and the correction or clarification relied upon, must be set forth in a

notice served on the plaintiff within 60 days after service of the [summons and complaint] or 10 days after the correction or clarification is made, whichever is later. A correction or clarification is deemed to be timely and sufficient unless the plaintiff challenges its timeliness or sufficiency within [20 days] after the notice is served.

(b) If a defendant in an action governed by this [Act] intends to challenge the adequacy or timeliness of a request for correction or clarification, the defendant must set forth the challenge in a motion to declare the request inadequate or untimely served within 60 days after service of the [summons and complaint]. The court shall rule on the motion at the earliest appropriate time before trial.

Section 8.
Offer to Correct or Clarify.

(a) If a timely correction or clarification is no longer possible, the publisher of an alleged defamatory statement may offer, at any time before trial, to make a correction or clarification. The offer must be made in writing to the person allegedly defamed by the publication and:

(1) contain the publisher's offer to:

(i) publish, at the person's request, a sufficient correction or clarification; and
(ii) pay the person's reasonable expenses of litigation, including attorney's fees, incurred before publication of the correction or clarification; and

(2) be accompanied by a copy of the proposed correction or clarification and the plan for its publication.

(b) If the person accepts in writing an offer to correct or clarify made pursuant to subsection (a):

(1) the person is barred from commencing an action against the publisher based on the statement; or
(2) if an action has been commenced, the court shall dismiss the action against the defendant with prejudice after the defendant complies with the terms of the offer.

(c) A person who does not accept an offer made in conformance with sub-

section (a) may recover in an action based on the statement only:

(1) damages for provable economic loss; and
(2) reasonable expenses of litigation, including attorney's fees, incurred before the offer, unless the person failed to make a good-faith attempt to request a correction or clarification in accordance with Section 3(b) or failed to disclose information in accordance with Section 4.

(d) On request of either party, a court shall promptly determine the sufficiency of the offered correction or clarification.

(e) The court shall determine the amount of reasonable expenses of litigation, including attorney's fees, specified in subsections (a)(1)(ii) and (c)(2).

Section 9.
Scope of Protection.

A timely and sufficient correction or clarification made by a person responsible for a publication constitutes a correction or clarification made by all persons responsible for that publication other than a republisher. However, a correction or clarification that is sufficient only because of the operation of Section 6(b)(2)(iii) does not constitute a correction or clarification made by the person to whom the statement is attributed.

Section 10.
Admissibility of Evidence of Correction or Clarification.

(a) The fact of a request for correction or clarification under this [Act], the contents of the request, and its acceptance or refusal are not admissible in evidence at trial.

(b) The fact that a correction or clarification under this [Act] was made and the contents of the correction or clarification are not admissible in evidence at trial except in mitigation of damages pursuant to Section 5. If the fact that a correction or clarification was made or the contents of the correction or clarification are received in evidence, the fact of the request may also be received.

(c) The fact of an offer of correction or clarification, or the fact of its refusal, and the contents of the offer are not admissible in evidence at trial.

Section 11.
Uniformity of Application and Construction.

This [Act] shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among States enacting it.

Section 12.
Short Title.

This [Act] may be cited as the Uniform Correction or Clarification of Defamation Act.

Section 13.
Severability.

If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act] which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

Section 14.
Effective Date.

This [Act] takes effect…

5. Alabama Retraction Statute

Alabama's Code § 6-5-186 on Prerequisites to recovery of vindictive or punitive damages in action for libel,

Vindictive or punitive damages shall not be recovered in any action for libel on account of any publication unless (1) it shall be proved that the publication was made by the defendant with knowledge that the matter published was false, or with reckless disregard of whether it was false or not, and (2) it shall be proved that five days before the commencement of the action the plaintiff shall have made written demand upon the defendant for a public retraction of the charge or matter published; and the defendant shall have failed or refused to publish within five days, in as prominent and public a place or manner as the charge or matter published occupied, a full and fair retraction of such charge or matter.

6. California Retraction Statute

California's Civil Code § 48a [Libel in newspaper; slander by radio broadcast]:

1. [Special damages; notice and demand for correction.]

In any action for damages for the publication of a libel in a newspaper, or of a slander by radio broadcast, plaintiff shall recover no more than special damages unless a correction be demanded and be not published or broadcast, as hereinafter provided. Plaintiff shall serve upon the publisher, at the place of publication or broadcaster at the place of broadcast, a written notice specifying the statements claimed to be libelous and demanding that the same be corrected. Said notice and demand must be served within 20 days after knowledge of the publication or broadcast of the statements claimed to be libelous.

2. [General, special and exemplary damages.]

If a correction be demanded within said period and be not published or broadcast in substantially as conspicuous a manner in said newspaper or on said broadcasting station as were the statements claimed to be libelous, in a regular issue thereof published or broadcast within three weeks after such service, plaintiff, if he pleads and proves such notice, demand and failure to correct, and if his cause of action be maintained, may recover general, special and exemplary damages; provided that no exemplary damages may be recovered unless the plaintiff shall prove that defendant made the publication or broadcast with actual malice and then only in the discretion of the court or jury, and actual malice shall not be inferred or presumed from the publication or broadcast.

3. [Correction prior to demand.]

A correction published or broadcast in substantially as conspicuous a manner in said newspaper or on said broadcasting station as the statements claimed in the complaint to be libelous, prior to receipt of a demand therefor, shall be of

the same force and effect as though such correction had been published or broadcast within three weeks after a demand therefor.

4. [Definitions.]

As used herein, the terms "general damages," "special damages," "exemplary damages" and "actual malice," are defined as follows:

a. "General damages" are damages for loss of reputation, shame, mortification and hurt feelings;
b. "Special damages" are all damages which plaintiff alleges and proves that he has suffered in respect to his property, business, trade, profession or occupation, including such amounts of money as the plaintiff alleges and proves he has expended as a result of the alleged libel, and no other;
c. "Exemplary damages" are damages which may in the discretion of the court or jury be recovered in addition to general and special damages for the sake of example and by way of punishing a defendant who has made the publication or broadcast with actual malice;
d. "Actual malice" is that state of mind arising from hatred or ill will toward the plaintiff; provided, however, that such a state of mind occasioned by a good faith belief on the part of the defendant in the truth of the libelous publication or broadcast at the time it is published or broadcast shall not constitute actual malice.

7. Chapter 22 of the Danish Civil Procedure Code

Unofficial translation by Henrik Spang-Hanssen of " Lov om rettens pleje" [1]

Consolidated Act no. 910 of 27 September 2005

Chapter Twenty-two on Jurisdiction

These rules are valid for lawsuits brought on or after 1 July 1986

Kapitel 22 - Stedlig kompetence	Chapter 22 - Local Jurisdiction
§235. Retssager anlægges ved sagsøgtes hjemting, medmindre andet er bestemt ved lov. **Stk. 2**. Hjemtinget er i den retskreds, hvor sagsøgte har bopæl. Har sagsøgte bopæl i flere retskredse, er hjemtinget i enhver af dem. **Stk. 3**. Har sagsøgte ingen bopæl, er hjemtinget i den retskreds, hvor han opholder sig. **Stk.4**. Har sagsøgte hverken bopæl eller kendt opholdssted, er hjemtinget i den retskreds, hvor han sidst har haft bopæl eller opholdssted.	**§235. Subsection 1**. Lawsuits are brought in the "home jurisdiction" of the defendant unless otherwise laid down by a specific statute. **Subsection 2**. The "home jurisdiction" of the defendant is the local jurisdiction where the defendant has permanent residence. If the defendant has permanent residence in several jurisdictions, the "home jurisdiction" shall be in each of these. **Subsection 3**. In case the defendant has no permanent residence, the "home jurisdiction" shall be the jurisdiction of the place where the defendant is staying. **Subsection 4**. If the defendant has neither a residence nor a known place of sojourn, the "home jurisdiction" shall be the jurisdiction, where the defendant last resided or stayed.
§236. Danske statsborgere, der er bosat i udlandet uden tillige at have bopæl i Danmark, og som ikke er undergivet bopælslandets domsmyndighed , har hjemting i København.	**§236**. Danish nationals domiciled outside Denmark without any residence in Denmark and without the jurisdiction of the country of residence have "home jurisdiction" in Copenhagen.
§237. Sager mod personer, der driver erhvervsmæssig virksomhed, kan, når sagen vedrører virksomheden, anlægges ved retten på det sted, hvorfra virksomheden udøves.	**§237**. Lawsuits against natural persons who run a business can be brought in the jurisdiction of the permanent place(s) of the business when the lawsuit concerns the business.
§238. Selskaber, foreninger, private institutioner og andre sammenslutninger, der kan optræde	**§238. Subsection 1**. Corporations, associations, private institutions and other kinds of organization

[1] U.K.: Administration of Justice Act

som part i retssager, har hjemting i den retskreds, hvor hovedkontoret ligger, eller, hvis et sådant ikke kan oplyses, i den retskreds, hvor et af bestyrelsens eller direktionens medlemmer har bopæl. **Stk. 2** Sager mod de i stk. 1 nævnte sammenslutninger, der driver erhvervsvirksomhed uden for hjemtinget, kan, når sagen vedrører virksomheden, anlægges ved retten på det sted, hvorfra virksomheden udøves. **Stk. 3**. Sager, der vedrører sammenslutningen, og som rejses af sammenslutningen mod de enkelte medlemmer eller opstår imellem disse, kan anlægges ved sammenslutningens hjemting. **Stk. 4**. Sager om erstatning mod stiftere, bestyrelsesmedlemmer og direktører i de i stk. 1 nævnte sammenslutninger kan anlægges ved sammenslutningens hjemting.	that can be a party to an action have "home jurisdiction" in the jurisdiction where the main office is located, or, if such is unknown, in the jurisdiction of the residence of a member of the board of directors or the executive board. **Subsection 2**. Lawsuits brought against organizations mentioned in subsection 1 that run business outside the "home jurisdiction" can be brought in the jurisdiction of the permanent place(s) of the business when the lawsuit concerns the business. **Subsection 3**. Lawsuits concerning an organization brought against the individual members or between these can be brought in the "home jurisdiction" of the organization. **Subsection 4**. Lawsuits concerning damages or compensation brought against a original subscriber to the memorandum of association of a company, members of the board of directors or the executive board can be brought at the court of the "home jurisdiction" of the organization.
§239. Kommuner har hjemting i den retskreds, hvor hovedkontoret ligger.	**§239**. The "home jurisdiction" of local authorities is the jurisdiction where the head office is located.
§240. Staten har hjemting i den retskreds, hvor den myndighed, som stævnes på statens vegne, har kontor. **Stk. 2**. Sager, som behandles ved landsret i 1. instans i medfør af §225, stk. 1, anlægges, hvor sagsøger har hjemting. Har sagsøger ikke hjemting i Danmark, anlægges sagen ved statens hjemting.	§240. Subsection 1. The "home jurisdiction" of the State is the jurisdiction of the office of the authority that the lawsuit concerns. **Subsection 2**. Lawsuits that begin at the Danish High Court as first instance pursuant to §225 subsection 1 shall be brought at the "home jurisdiction" of the defendant. If the defendant has no "home jurisdiction" in Denmark, the lawsuit shall be brought at the "home jurisdiction" of the State.
§241. Sager vedrørende rettigheder over fast ejendom kan anlægges ved retten på det sted, hvor ejendommen ligger.	**§241**. Lawsuits concerning rights [overing more than title] to real estate can be brought at the jurisdiction of the estate.
§242. Sager om kontraktsforhold kan anlægges ved retten på det sted, hvor den forpligtelse, der ligger til grund for sagen, er opfyldt eller skal opfyldes. **Stk. 2**. Bestemmelsen i stk. 1 finder ikke anvendelse på pengekrav, medmindre kravet er opstået under ophold i retskredsen under sådanne omstændigheder, at det skulle opfyldes, inden stedet forlades.	**§242. Subsection** 1. Lawsuits concerning contracts can be brought at the place where the obligation or responsibility on which the claim is based has been or should be fulfilled. **Subsection 2**. Subsection 1 does not apply to pecuniary claims unless the claim arose while the defendant stayed in the jurisdiction and the obligation or responsibility was to be fulfilled before his leaving the jurisdiction.
§243. Sager, hvorunder der påstås straf, erstatning eller oprejsning i anledning af retskrænkelser, kan anlægges ved retten på det sted, hvor retskrænkelsen er foregået.	**§243**. Lawsuits concerning breach of law involving claim of penalty, damages or redress of a wrong can be brought in the jurisdiction of the location where the breach of law took place.
§244. I sager om forbrugeraftaler, som ikke er indgået ved personlig henvendelse på den erhvervsdrivendes faste forretningssted, kan forbrugeren anlægge sag mod den erhvervsdrivende ved sit eget hjemting.	**§244**. Lawsuits concerning consumer contracts that are not entered into by the consumer at the permanent place of the business can be brought against the business at the "home jurisdiction" of the consumer.

§245 Parterne kan aftale, ved hvilken af flere ligeartede retter sagen skal anlægges. **Stk. 2**. I sager om forbrugeraftaler er en forudgående aftale om værneting ikke bindende for forbrugeren.	**§245. Subsection 1**. The parties may agree at which court, among courts at the same level, lawsuits can be brought. **Subsection 2**. In lawsuits concerning consumer contracts, an agreement is only valid if entered into after the dispute has arisen.
§246. Sager mod personer, selskaber, foreninger, private institutioner og andre sammenslutninger, der ikke har hjemting i Danmark, kan anlægges her i landet, for så vidt nogen ret efter bestemmelserne i §§ 237, 238, stk. 2, 241, 242, 243 og 245 kan anses som værneting i sagen. I sager om forbrugeraftaler kan forbrugeren anlægge sag mod de i 1. pkt. nævnte personer og sammenslutninger ved sit eget hjemting, såfremt fremsættelsen af særligt tilbud eller reklamering i Danmark er gået forud for aftalens indgåelse og forbrugeren her i landet har foretaget de dispositioner, der er nødvendige til indgåelse af aftalen. **Stk. 2**. Kan ingen ret efter stk. 1 anses som værneting i sagen, kan sager vedrørende formueretsforhold mod de i stk. 1 nævnte personer anlægges ved retten på det sted, hvor de ved stævningens forkyndelse opholder sig. **Stk. 3**. Sager vedrørende formueretsforhold mod de i stk. 1 nævnte personer og sammenslutninger kan endvidere, hvis der ikke er værneting efter reglen i stk. 1, anlægges ved retten på det sted, hvor den pågældende person eller sammenslutning på tidspunktet for sagens anlæg har gods, eller hvor det gods, kravet angår, befinder sig på tidspunktet for sagens anlæg. Afværges arrest i gods gennem sikkerhedsstillelse, betragtes sikkerhedsstillelsen som gods, der befinder sig på det sted, hvor arrestbegæringen er eller i givet fald skulle være indgivet.	**§246. Subsection 1**. Lawsuits against persons, corporations, associations, private institutions and other kinds of organization that does not have “home jurisdiction” in Denmark can be brought in Denmark if any court pursuant to §§ 237, 238, subsections 2, 241, 242, 243 and 245 can be regarded as jurisdiction for the case. In lawsuits concerning consumer contracts, the consumer can bring a lawsuit against the said persons and organizations at the consumers “home jurisdiction” if a special offer or advertising in Denmark was made before the agreement was entered into and the necessary actions for the fulfillment of the agreement were made by the consumer in Denmark. **Subsection 2**. If no court can be regarded as having jurisdiction in the case pursuant to subsection 1, then lawsuits concerning financial circumstances against the persons mentioned in subsection 1 can be brought at the court at the place, where the [natural] person stayed at the time of service of process. **Subsection 3**. If there is no jurisdiction according to subsection 1, lawsuits concerning financial circumstances against the persons and organizations mentioned in subsection 1 can be brought at court at the place where the defendant has property at the time of filing the suit or where the property that the dispute concerns is located at the time when the suit is filed. If arrest of property (as an interim remedy) is avoided by giving security, the security is regarded as property located where the application for attachment was or should have been filed.
§246a. Sager om stadfæstelse af arrest i et skib og om den fordring, for hvilken arresten er gjort, kan anlægges ved retten på det sted, hvor arresten er foretaget eller ville være foretaget, hvis den ikke var afværget ved sikkerhedsstillelse.	**§246a**. Lawsuits concerning the confirmation of arrest, as an interim remedy, of a vessel and concerning the claim that was the basis for the arrest can be brought at the court at the place where the arrest was, and, if security had not been given, could have been made.
§247. I sager, der er omfattet af en konvention, som er gennemført i dansk ret ved lov om EF-domskonventionenm.v., herunder ved bekendtgørelse i medfør af den nævnte lovs §15, anvendes konventionens værnetingsregler. Dette gælder dog ikke sager, der anlægges ved det i §246 a nævnte værneting, og som er omfattet af konventionen af 10. maj 1952 om arrest i søgående skibe. **Stk. 2**. Hvor der ikke efter dansk lovgivning i øvrigt er værneting for en sag, der efter en	**§247**. Subsection 1. In lawsuits covered by a convention implemented in Danish law by the EU judgment convention Act [= Bruxelles Convention], among other things by executive order pursuant to §15 of that Act, the rules by that Act are used, unless the lawsuit is filed pursuant to §246a and covered by the Convention on seizure of seagoing vessels of 10 May 1952. **Subsection 2**. In cases where Danish law does not provide jurisdiction for a lawsuit which, pursuant to a convention mentioned in subsection 1, first sentence,

konvention som nævnt i stk.1, 1. pkt., skal eller kan anlægges her i landet, anlægges sagen ved sagsøgerens hjemting eller, såfremt sagsøgeren ikke har hjemting her i landet, ved Københavns Byret eller Østre Landsret.	can or has to be filed in Denmark, the lawsuit can be brought at the plaintiff's "home jurisdiction" or, if the plaintiff does not have any "home jurisdiction", at the Copenhagen City Court or Eastern Division of the Danish High Court.
§248. Retten påser af egen drift, om sagen er indbragt for rette værneting. Fremsætter sagsøgte ikke indsigelse mod rettens kompetence i svarskriftet eller, hvis sagen ikke forberedes skriftligt, i det 1. retsmøde under forberedelsen, anses retten for rette værneting. **Stk. 2**. Er sagen anlagt ved en ret, som ikke er rette værneting til at behandle sagen eller et af de rejste krav, henviser retten om muligt sagen eller kravet til afgørelse ved rette domstol. Afgørelse om henvisning træffes ved kendelse. Kan henvisning ikke ske, afviser retten sagen ved dom.	**§248. Subsection 1**. The court ensures ex officio that the lawsuit is brought at the competent jurisdiction. If the defendant does not make any objection to the competence of the court in the first statement of defense, or in the case of preliminary proceedings, objections were not made in writing at the first pre-trial procedure, the court is regarded as the correct jurisdiction. **Subsection 2**. If the lawsuit is filed at a court that does not have jurisdiction or cannot deal with one of the claims, if possible the court shall transfer the case or the claim to the correct court. A decision of transfer is done in the form of a court order. If transfer is not allowed, the court shall dismiss the lawsuit by a judgment.

8. Parallel Treaty on jurisdiction between Denmark and the rest of the E.U.

O.J. L299, 16.11.2005, p. 0061

COUNCIL

COUNCIL DECISION of 20 September 2005

on the signing, on behalf of the Community, of the Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (2005/790/EC)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 61(c) thereof, in conjunction with the first sentence of the first subparagraph of Article 300(2) thereof,

Having regard to the proposal from the Commission,

Whereas:

(1) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and the Treaty establishing the European Community, Denmark is not bound by the provisions of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters1 (1), nor subject to their application.

[1] OJ L 12, 16.1.2001, p. 1. Regulation as last amended by Commission Regulation (EC) No 2245/2004 (OJ. L 381, 28.12.2004, p. 10).

(2) By Decision of 8 May 2003, the Council authorised exceptionally the Commission to negotiate an agreement between the European Community and the Kingdom of Denmark extending to Denmark the provisions of the abovementioned Regulation.

(3) The Commission has negotiated such agreement, on behalf of the Community, with the Kingdom of Denmark.

(4) The United Kingdom and Ireland, in accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and the Treaty establishing the European Community, are taking part in the adoption and application of this Decision.

(5) In accordance with Articles 1 and 2 of the abovementioned Protocol on the position of Denmark, Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application.

(6) The Agreement, initialled at Brussels on 17 January 2005, should be signed,

HAS DECIDED AS FOLLOWS:

Article 1

The signing of the Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters is hereby approved on behalf of the Community, subject to the Council Decision concerning the conclusion of the said Agreement.

The text of the Agreement is attached to this Decision.

Article 2

The President of the Council is hereby authorised to designate the person(s) empowered to sign the Agreement on behalf of the Community subject to its conclusion.

Done at Brussels, 20 September 2005.

For the Council

The President

O.J, L 299, 16.11.2005, p. 0062-0070

AGREEMENT

between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

THE EUROPEAN COMMUNITY, hereinafter referred to as 'the Community',

of the one part, and

THE KINGDOM OF DENMARK, hereinafter referred to as 'Denmark',

of the other part,

DESIRING to unify the rules of conflict of jurisdiction in civil and commercial matters and to simplify the formalities with a view to rapid and simple recognition and enforcement of judgments within the Community,

WHEREAS on 27 September 1968 the Member States, acting under Article 293, fourth indent, of the Treaty establishing the European Community, concluded the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters2 (the Brussels Convention), as amended by Conventions on the Accession of the new Member States to that Convention. On 16 September 1988 the Member States and the EFTA States concluded the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters3 (the Lugano Convention), which is a parallel Convention to the Brussels Convention,

[2] O.J. L 299, 31.12.1972, p. 32; O.J. L 304, 30.10.1978, p. 1; O.J. L 388, 31.12.1982, p. 1; O.J. L 285, 3.10.1989, p. 1; OJ C 15, 15.1.1997, p. 1. For a consolidated text, see O.J. C 27, 26.1.1998, p. 1.

[3] O.J. L 319, 25.11.1988, p. 9.

WHEREAS the main content of the Brussels Convention has been taken over in Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters4 (the Brussels I Regulation),

REFERRING to the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty establishing the European Community (the Protocol on the position of Denmark) pursuant to which the Brussels I Regulation shall not be binding upon or applicable in Denmark,

STRESSING that a solution to the unsatisfactory legal situation arising from differences in applicable rules on jurisdiction, recognition and enforcement of judgments within the Community must be found,

DESIRING that the provisions of the Brussels I Regulation, future amendments thereto and the implementing measures relating to it should under international law apply to the relations between the Community and Denmark being a Member State with a special position with respect to Title IV of the Treaty establishing the European Community,

STRESSING that continuity between the Brussels Convention and this Agreement should be ensured, and that transitional provisions as in the Brussels I Regulation should be applied to this Agreement as well. The same need for continuity applies as regards the interpretation of the Brussels Convention by the Court of Justice of the European Communities and the 1971 Protocol5 should remain applicable also to cases already pending when this Agreement enters into force,

STRESSING that the Brussels Convention also continues to apply to the territories of the Member States which fall within the territorial scope of that

[4] O.J. L 12, 16.1.2001, p. 1. Regulation as last amended by Commission Regulation (EC) No 2245/2004 (O.J. L 381, 28.12.2004, p. 10).

[5] O.J. L 204, 2.8.1975, p. 28; O.J. L 304, 30.10.1978, p. 1; O.J. L 388, 31.12.1982, p. 1; O.J. L 285, 3.10.1989, p. 1; O.J. C 15, 15.1.1997, p. 1. For a consolidated text see O.J. C 27, 26.1.1998, p. 28.

Convention and which are excluded from this Agreement,

STRESSING the importance of proper coordination between the Community and Denmark with regard to the negotiation and conclusion of international agreements that may affect or alter the scope of the Brussels I Regulation,

STRESSING that Denmark should seek to join international agreements entered into by the Community where Danish participation in such agreements is relevant for the coherent application of the Brussels I Regulation and this Agreement,

STATING that the Court of Justice of the European Communities should have jurisdiction in order to secure the uniform application and interpretation of this Agreement including the provisions of the Brussels I Regulation and any implementing Community measures forming part of this Agreement,

REFERRING to the jurisdiction conferred to the Court of Justice of the European Communities pursuant to Article 68(1) of the Treaty establishing the European Community to give rulings on preliminary questions relating to the validity and interpretation of acts of the institutions of the Community based on Title IV of the Treaty, including the validity and interpretation of this Agreement, and to the circumstance that this provision shall not be binding upon or applicable in Denmark, as results from the Protocol on the position of Denmark,

CONSIDERING that the Court of Justice of the European Communities should have jurisdiction under the same conditions to give preliminary rulings on questions concerning the validity and interpretation of this Agreement which are raised by a Danish court or tribunal, and that Danish courts and tribunals should therefore request preliminary rulings under the same conditions as courts and tribunals of other Member States in respect of the interpretation of the Brussels I Regulation and its implementing measures,

REFERRING to the provision that, pursuant to Article 68(3) of the Treaty establishing the European Community, the Council of the European Union, the European Commission and the Member States may request the Court of Justice of the European Communities to give a ruling on the interpretation of acts of the institutions of the Community based on Title IV of the Treaty, including the interpretation of this Agreement, and the circumstance that this provision shall not be binding upon or applicable in Denmark, as results from

the Protocol on the position of Denmark,

CONSIDERING that Denmark should, under the same conditions as other Member States in respect of the Brussels I Regulation and its implementing measures, be accorded the possibility to request the Court of Justice of the European Communities to give rulings on questions relating to the interpretation of this Agreement,

STRESSING that under Danish law the courts in Denmark should, when interpreting this Agreement including the provisions of the Brussels I Regulation and any implementing Community measures forming part of this Agreement, take due account of the rulings contained in the case law of the Court of Justice of the European Communities and of the courts of the Member States of the European Communities in respect of provisions of the Brussels Convention, the Brussels I Regulation and any implementing Community measures,

CONSIDERING that it should be possible to request the Court of Justice of the European Communities to rule on questions relating to compliance with obligations under this Agreement pursuant to the provisions of the Treaty establishing the European Community governing proceedings before the Court,

WHEREAS, by virtue of Article 300(7) of the Treaty establishing the European Community, this Agreement binds Member States; it is therefore appropriate that Denmark, in the case of non-compliance by a Member State, should be able to seize the Commission as guardian of the Treaty,

HAVE AGREED AS FOLLOWS:

Article 1
Aim

1. The aim of this Agreement is to apply the provisions of the Brussels I Regulation and its implementing measures to the relations between the Community and Denmark, in accordance with Article 2(1) of this Agreement.

2. It is the objective of the Contracting Parties to arrive at a uniform application and interpretation of the provisions of the Brussels I Regulation and its implementing measures in all Member States.

3. The provisions of Articles 3(1), 4(1) and 5(1) of this Agreement result from the Protocol on the position of Denmark.

Article 2
Jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

1. The provisions of the Brussels I Regulation, which is annexed to this Agreement and forms part thereof, together with its implementing measures adopted pursuant to Article 74(2) of the Regulation and, in respect of implementing measures adopted after the entry into force of this Agreement, implemented by Denmark as referred to in Article 4 of this Agreement, and the measures adopted pursuant to Article 74(1) of the Regulation, shall under international law apply to the relations between the Community and Denmark.

2. However, for the purposes of this Agreement, the application of the provisions of that Regulation shall be modified as follows:

(a) Article 1(3) shall not apply.

(b) Article 50 shall be supplemented by the following paragraph (as paragraph 2):

> '2. However, an applicant who requests the enforcement of a decision given by an administrative authority in Denmark in respect of a maintenance order may, in the Member State addressed, claim the benefits referred to in the first paragraph if he presents a statement from the Danish Ministry of Justice to the effect that he fulfils the financial requirements to qualify for the grant of complete or partial legal aid or exemption from costs or expenses.'

(c) Article 62 shall be supplemented by the following paragraph (as paragraph 2):

> '2. In matters relating to maintenance, the expression "court" includes the Danish administrative authorities.'

(d) Article 64 shall apply to seagoing ships registered in Denmark as well as in Greece and Portugal.

(e) The date of entry into force of this Agreement shall apply instead of the date of entry into force of the Regulation as referred to in Articles 70(2), 72 and 76 thereof.

(f) The transitional provisions of this Agreement shall apply instead of Article 66 of the Regulation.

(g) In Annex I the following shall be added: 'in Denmark: Article 246(2) and (3) of the Administration of Justice Act (lov om rettens pleje)'.

(h) In Annex II the following shall be added: 'in Denmark, the "byret…

(i) In Annex III the following shall be added: 'in Denmark, the "landsret"'.

(j) In Annex IV the following shall be added: 'in Denmark, an appeal to the "Højesteret" with leave from the 'Procesbevillingnævnet"'.

Article 3
Amendments to the Brussels I Regulation

1. Denmark shall not take part in the adoption of amendments to the Brussels I Regulation and no such amendments shall be binding upon or applicable in Denmark.

2. Whenever amendments to the Regulation are adopted Denmark shall notify the Commission of its decision whether or not to implement the content of such amendments. Notification shall be given at the time of the adoption of the amendments or within 30 days thereafter.

3. If Denmark decides that it will implement the content of the amendments the notification shall indicate whether implementation can take place administratively or requires parliamentary approval.

4. If the notification indicates that implementation can take place administratively the notification shall, moreover, state that all necessary administrative measures enter into force on the date of entry into force of the amendments to

the Regulation or have entered into force on the date of the notification, whichever date is the latest.

5. If the notification indicates that implementation requires parliamentary approval in Denmark, the following rules shall apply:

(a) Legislative measures in Denmark shall enter into force on the date of entry into force of the amendments to the Regulation or within 6 months after the notification, whichever date is the latest;

(b) Denmark shall notify the Commission of the date upon which the implementing legislative measures enter into force.

6. A Danish notification that the content of the amendments has been implemented in Denmark, in accordance with paragraphs 4 and 5, creates mutual obligations under international law between Denmark and the Community. The amendments to the Regulation shall then constitute amendments to this Agreement and shall be considered annexed hereto.

7. In cases where:

(a) Denmark notifies its decision not to implement the content of the amendments; or

(b) Denmark does not make a notification within the 30-day time-limit set out in paragraph 2; or

(c) Legislative measures in Denmark do not enter into force within the time-limits set out in paragraph 5,

this Agreement shall be considered terminated unless the parties decide otherwise within 90 days or, in the situation referred to under (c), legislative measures in Denmark enter into force within the same period. Termination shall take effect three months after the expiry of the 90-day period.

8. Legal proceedings instituted and documents formally drawn up or registered as authentic instruments before the date of termination of the Agreement as set out in paragraph 7 are not affected hereby.

Article 4
Implementing measures

1. Denmark shall not take part in the adoption of opinions by the Committee referred to in Article 75 of the Brussels I Regulation. Implementing measures adopted pursuant to Article 74(2) of that Regulation shall not be binding upon and shall not be applicable in Denmark.

2. Whenever implementing measures are adopted pursuant to Article 74(2) of the Regulation, the implementing measures shall be communicated to Denmark. Denmark shall notify the Commission of its decision whether or not to implement the content of the implementing measures. Notification shall be given upon receipt of the implementing measures or within 30 days thereafter.

3. The notification shall state that all necessary administrative measures in Denmark enter into force on the date of entry into force of the implementing measures or have entered into force on the date of the notification, whichever date is the latest.

4. A Danish notification that the content of the implementing measures has been implemented in Denmark creates mutual obligations under international law between Denmark and the Community. The implementing measures will then form part of this Agreement.

5. In cases where:

(a) Denmark notifies its decision not to implement the content of the implementing measures; or

(b) Denmark does not make a notification within the 30-day time-limit set out in paragraph 2,

this Agreement shall be considered terminated unless the parties decide otherwise within 90 days. Termination shall take effect three months after the expiry of the 90-day period.

6. Legal proceedings instituted and documents formally drawn up or registered as authentic instruments before the date of termination of the Agreement as set out in paragraph 5 are not affected hereby.

7. If in exceptional cases the implementation requires parliamentary approval in Denmark, the Danish notification under paragraph 2 shall indicate this and the provisions of Article 3(5) to (8) shall apply.

8. Denmark shall notify the Commission of texts amending the items set out in Article 2(2)(g) to (j) of this Agreement. The Commission shall adapt Article 2(2)(g) to (j) accordingly.

Article 5
International agreements which affect the Brussels I Regulation

1. International agreements entered into by the Community based on the rules of the Brussels I Regulation shall not be binding upon and shall not be applicable in Denmark.

2. Denmark will abstain from entering into international agreements which may affect or alter the scope of the Brussels I Regulation as annexed to this Agreement unless it is done in agreement with the Community and satisfactory arrangements have been made with regard to the relationship between this Agreement and the international agreement in question.

3. When negotiating international agreements that may affect or alter the scope of the Brussels I Regulation as annexed to this Agreement, Denmark will coordinate its position with the Community and will abstain from any actions that would jeopardise the objectives of a Community position within its sphere of competence in such negotiations.

Article 6
Jurisdiction of the Court of Justice of the European Communities in relation to the interpretation of the Agreement

1. Where a question on the validity or interpretation of this Agreement is raised in a case pending before a Danish court or tribunal, that court or tribunal shall request the Court of Justice to give a ruling thereon whenever under the same circumstances a court or tribunal of another Member State of the European Union would be required to do so in respect of the Brussels I Regulation and its implementing measures referred to in Article 2(1) of this

Agreement.

2. Under Danish law, the courts in Denmark shall, when interpreting this Agreement, take due account of the rulings contained in the case law of the Court of Justice in respect of provisions of the Brussels Convention, the Brussels I Regulation and any implementing Community measures.

3. Denmark may, like the Council, the Commission and any Member State, request the Court of Justice to give a ruling on a question of interpretation of this Agreement. The ruling given by the Court of Justice in response to such a request shall not apply to judgments of courts or tribunals of the Member States which have become res judicata.

4. Denmark shall be entitled to submit observations to the Court of Justice in cases where a question has been referred to it by a court or tribunal of a Member State for a preliminary ruling concerning the interpretation of any provision referred to in Article 2(1).

5. The Protocol on the Statute of the Court of Justice of the European Communities and its Rules of Procedure shall apply.

6. If the provisions of the Treaty establishing the European Community regarding rulings by the Court of Justice are amended with consequences for rulings in respect of the Brussels I Regulation, Denmark may notify the Commission of its decision not to apply the amendments in respect of this Agreement. Notification shall be given at the time of the entry into force of the amendments or within 60 days thereafter.

In such a case this Agreement shall be considered terminated. Termination shall take effect three months after the notification.

7. Legal proceedings instituted and documents formally drawn up or registered as authentic instruments before the date of termination of the Agreement as set out in paragraph 6 are not affected hereby.

Article 7
Jurisdiction of the Court of Justice of the European Communities in relation to compliance with the Agreement

1. The Commission may bring before the Court of Justice cases against Denmark concerning non-compliance with any obligation under this Agreement.

2. Denmark may bring a complaint before the Commission as to the non-compliance by a Member State of its obligations under this Agreement.

3. The relevant provisions of the Treaty establishing the European Community governing proceedings before the Court of Justice as well as the Protocol on the Statute of the Court of Justice of the European Communities and its Rules of Procedure shall apply.

Article 8
Territorial application

1. This Agreement shall apply to the territories referred to in Article 299 of the Treaty establishing the European Community.

2. If the Community decides to extend the application of the Brussels I Regulation to territories currently governed by the Brussels Convention, the Community and Denmark shall cooperate in order to ensure that such an application also extends to Denmark.

Article 9
Transitional provisions

1. This Agreement shall apply only to legal proceedings instituted and to documents formally drawn up or registered as authentic instruments after the entry into force thereof.

2. However, if the proceedings in the Member State of origin were instituted before the entry into force of this Agreement, judgments given after that date shall be recognised and enforced in accordance with this Agreement,

(a) if the proceedings in the Member State of origin were instituted after the

entry into force of the Brussels or the Lugano Convention both in the Member State of origin and in the Member State addressed;

(b) in all other cases, if jurisdiction was founded upon rules which accorded with those provided for either in this Agreement or in a convention concluded between the Member State of origin and the Member State addressed which was in force when the proceedings were instituted.

Article 10
Relationship to the Brussels I Regulation

1. This Agreement shall not prejudice the application by the Member States of the Community other than Denmark of the Brussels I Regulation.

2. However, this Agreement shall in any event be applied:

(a) in matters of jurisdiction, where the defendant is domiciled in Denmark, or where Article 22 or 23 of the Regulation, applicable to the relations between the Community and Denmark by virtue of Article 2 of this Agreement, confer jurisdiction on the courts of Denmark;

(b) in relation to a lis pendens or to related actions as provided for in Articles 27 and 28 of the Brussels I Regulation, applicable to the relations between the Community and Denmark by virtue of Article 2 of this Agreement, when proceedings are instituted in a Member State other than Denmark and in Denmark;

(c) in matters of recognition and enforcement, where Denmark is either the State of origin or the State addressed.

Article 11
Termination of the agreement

1. This Agreement shall terminate if Denmark informs the other Member States that it no longer wishes to avail itself of the provisions of Part I of the Protocol on the position of Denmark, in accordance with Article 7 of that Protocol.

2. This Agreement may be terminated by either Contracting Party giving notice to the other Contracting Party. Termination shall be effective six months after the date of such notice.

3. Legal proceedings instituted and documents formally drawn up or registered as authentic instruments before the date of termination of the Agreement as set out in paragraph 1 or 2 are not affected hereby.

Article 12
Entry into force

1. The Agreement shall be adopted by the Contracting Parties in accordance with their respective procedures.

2. The Agreement shall enter into force on the first day of the sixth month following the notification by the Contracting Parties of the completion of their respective procedures required for this purpose.

Article 13
Authenticity of texts

This Agreement is drawn up in duplicate in the Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Slovene, Slovak, Spanish and Swedish languages, each of these texts being equally authentic.

Done at Brussels on the nineteenth day of October in the year two thousand and five.

For the European Community / For the Kingdom of Denmark

ANNEX

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, as amended by Commission Regulation (EC) No 1496/2002 of 21

August 2002 amending Annex I (the rules of jurisdiction referred to in Article 3(2) and Article 4(2)) and Annex II (the list of competent courts and authorities) to Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters and by Commission Regulation (EC) No 2245/2004 of 27 December 2004 amending Annexes I, II, III and IV to Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

9. Denmark's Reservations to the Cybercrime Convention and its Protocol

Convention

Denmark's Reservation contained in the instrument of ratification deposited on 21 June 2005:

<http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=11&DF=7/25/2006&CL=ENG&VL=1> (visited 24 July 2006)

In accordance with Article 9, paragraph 4, of the Convention, the Government of the Kingdom of Denmark declares that the criminal area according to **Article 9** shall not comprehend the possession of obscene pictures of a person attained the age of fifteen, if the person concerned has given his or her consent to the possession, cf. Article 9, paragraph 1, letter e.
Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 9

In accordance with Article 9, paragraph 4, of the Convention, the Government of the Kingdom of Denmark declares that the criminal area according to **Article 9** shall not comprehend visual representations of a person appearing to be a minor engaged in sexually explicit conduct, cf. Article 9, paragraph 2, letter b.
Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 9

In accordance with Article 14, paragraph 3, letter a,of the Convention, the Government of the Kingdom of Denmark declares that Denmark will only apply **article 20** concerning monitoring of traffic data to the extent where in accordance with Article 21 there is an obligation to empower the competent authorities to monitor content data, in relation to inquiries of serious crimes, as defined by national law.
Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 14

Pursuant to **Article 38** of the Convention, Denmark declares that, until further notice, the Convention will not apply to the Feroe Islands and Greenland.

Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 38

ooo000ooo

Declarations contained in a letter from the Permanent Representative of Denmark, dated 28 September 2005, registered at the Secretariat General on 30 September 2005:

In accordance with Article 24, paragraph 7, of the Convention, the Government of the Kingdom of Denmark has designated the Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark, as competent authority.
Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 24

In accordance with Article 27, paragraph 2, of the Convention, the Government of the Kingdom of Denmark has designated the Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark, as competent authority.
Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 27

In accordance with Article 35, paragraph 1, of the Convention, the Government of the Kingdom of Denmark has designated the Danish National Police, Police Department, Polititorvet 14, DK-1780 Copenhagen V, Denmark, as competent authority.
Period covered: 1/10/2005 -
The preceding statement concerns Article(s) : 35

#########

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

<http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=189&CM=11&DF=7/25/2006&CL=ENG&VL=1> (visited 24 July 2006)

Reservation contained in the instrument of ratification deposited on 21 June 2005 and confirmed in a letter from the Deputy Permanent Representative of Denmark, dated 13 June 2006, registered at the Secretariat General on 15 June 2006:

In accordance with Article 3, paragraphs 2 and 3, of the Protocol, the Government of the Kingdom of Denmark declares that Denmark reserves the right to fully or to partially refrain from criminalising acts covered by **Article 3, paragraph 1**.
Period covered: 1/3/2006 -
The preceding statement concerns Article(s) : 3

In accordance with Article 5, paragraph 2, letter b, of the Protocol, the Government of the Kingdom of Denmark declares that Denmark reserves the right to fully or to partially refrain from criminalising acts covered by **Article 5, paragraph 1**.
Period covered: 1/3/2006 -
The preceding statement concerns Article(s) : 5

In accordance with Article 6, paragraph 2, letter b, of the Protocol, the Government of the Kingdom of Denmark declares that Denmark reserves the right to fully or to partially refrain from criminalising acts covered by **Article 6, paragraph 1**.
Period covered: 1/3/2006 -
The preceding statement concerns Article(s) : 6

ooo000ooo

Declaration contained in the instrument of ratification deposited on 21 June 2005:

Pursuant to Article 14 of the Protocol, Denmark declares, until further notice, the Protocol will not apply to the Feroe Islands and Greenland.
Period covered: 1/3/2006 -
The preceding statement concerns Article(s) : 14

10. Abbreviations

[see also through Index]

Danish case citation form: <"UfR" "year.page" "abbreviation in court hierarchy">:

5. Ø = Easter Appeal Court - Østre Landsret
6. V = Western Appeal Court - Vestre Landsret
7. SH = The Maritime and Commercial Court - Sø- og Handelsretten i København
8. H = Supreme Court of Denmark – Højesteret - Information in English at <www.hoejesteret.dk/?id=303>
9. No letter = lowest Danish court (but not necessary being first instance court)

E.F. Tidende - Official Journal of European Union

E.U. Tidende – Official Journal of European Union

EF-domskonventionen – E.U. Civil Jurisdiction Convention

F.T. – see Folketings Tidende

Folketings Tidende (F.T.) - Official Journal of parliamentary proceedings

Journal of Law – part B of UfR

Juristen - A major Danish Magazine containing articles on law and economic

Karnov Lovsamling – [Karnov statute book] (Karnov Publishing (a Thompson company)

O.J. – Official Journal of European Union [E.U. Tidende / E.F. Tidende]

Ophavsretloven – Danish Copyright Act

Retsplejeloven (Rpl.) - Danish Civil Procedure Code [UK: Administration of Justice Act] - Unofficial translation by Henrik Spang-Hanssen of Chapter 22 on Civil Jurisdiction at <http://www.geocities.com/hssph/Chapter22.htm>

RFC – Request for Comments

Rpl. – see Retsplejeloven

SHT - Case Reporter of Maritime and Commercial Court in Copenhagen

Straffeloven - Danish Civil Penal Code [or Criminal Code]

UfR – see Ugeskrift for Retsvæsen

Ugeskrift for Retsvæsen - (Part A) Danish Case Reporter or (Part B) Journal of Law, see further "Danish case citation form" above

VLT - Case Reporter of Western Appeal Court of Denmark

11. Bibliography

A Note on the Internet, Graduate School of Business, Stanford University 1996, at <www.stanford.edu/group/scip/Afeche-internet.pdf> (visited December 21, 2005)

Aboba, B. & W. Dixon, IPsec-Network Address Translation (NAT) Compatibility Requirements, RFC 3715 (March 2004)

Ad Hoc Committee on the Elaboration of a Convention against Transnational Organized Crime on the work of its first to eleventh sessions, - Report, U.N. Doc. A/55/383/Add.1 of 3 November 2000 at <www.unodc.org/unodc/en/crime_cicp_convention_dociments.html> file 383a1e.pdf

Addis, Adeno, The Thin State in Thick Globalism: Sovereignty in the Information Age, 37 Vanderbilt Journal of Transnational Law 1 (2004)

AFP, Appeal court to try former Yahoo! boss in Nazi memorabilia case, AFP, March 17, 2004 at <http://uk.news.yahoo.com/040317/eotuk.html>

AFP, French prosecutor argues for no sentence for former Yahoo! boss on trial, Yahoo! News Singapore, January 8, 2003, at <http://sg.news.yahoo.com/030107/1/36ajx.html (visited January 8, 2003)

Agreement Relating to the International Telecommunications Satellite Organization "INTELSAT", done at Washington August 20, 1971 (into force February 12, 1973) with annexes and Operating Agreement at <http://www.islandone.org/Treaties/BH585.html> (visited July 2006)

Akehurst, Michael, Jurisdiction in International Law, 46 Brit.Y.Int'L (1972-73) 145

Allott, Philip, The Health of Nations: Society and the Law Beyond States (2002 - ISBN 0521016800)

Almquist, Type of Service in the Internet Protocol Suite, RFC 1349 (July 1992)

American Bar Association, Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues created by the Internet, 55 Buslaw 1801 (August 2000)

American Jurisprudence on Commerce, 2nd Ed West Publishing

Amici Brief from Center for Democracy and Technology, American Civil Liberties Union, Electronic Frontier Foundation, Human Rights Watch et. al. - in the Yahoo ctr LICRA case, 2002 WL 32302224

Amici Curiae Brief of September 13 2004 in the Yahoo ctr LICRA case at <http://www.cdt.org/jurisdiction/20040921amici.pdf> (visited September 26, 2004

Amicus Brief from the European Commission in Support of Neither Party of January 23, 2004 on Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit in Soda v. Alvarez-Machain et. al., 2004 WL 177036 (U.S.)

Amnesty International, Universal Jurisdiction (2001) (AI Index: IOR 53/003/2001) at <www.amnesty.org> or <www.iccnow.org>

Andersen, Jens Anker, Kreditorforfølgning mod kontantindeståender i pengeinstitutter [Execution into cash deposits in financial institution], Juristen 1972.433

Andersen, Mads Bryde, Förändres juristens arbetsmetoder? i Edb, lovgivningen og juristenes rolle: Nordisk årbok i rettsinformatikk 1990 page 116-117

Andersen, Mads Bryde, IT-retten [(Danish) IT law] (Forlaget IT-retten [IT-law Publishing], Copenhagen, 1. Ed. - ISBN 87-988580-0-0-9), also at <www.it-retten.dk> (in Danish)

Andersen, Paul Krüger, m.fl., Dansk Privatret (12. Ed., DJØF Publishing 2001)

Annan, Kofi, Two concepts of sovereignty, The Economist, 18 September 1999, at <http://www.un.org/News/ossg/sg/stories/kaecon.html> (visited January 12, 2006)

Anonymizer's which effectively cloak IP addresses from mapping applications "PrivateSurfing" at <http://www. anonymizer.com/privatesurfing> (visited 14 October 2003)

Atkinson, IP Authentication Header, RFC 1826 (August 1995)

Atkinson, IP Encapsulating Security Payload (ESP), RFC 1827, (August 1995)

Atkinson, Security Architecture for the Internet Protocol, RFC 1825 (August 1995)

Australian, Gutnick 'delight' on defamation deal, The Australian, November 12, 2004 at <http://www.theaustralian.news.com.au/common/story_page/0,5744,11365187%255E1702,00.html> (visited November 15, 2004)

Baker (Ed.), Requirements for IP Version 4 Routers, RFC 1812 (1995)

Barakat, Matthew, Judge Sentences Spammer to Nine Years, AP 2 April 2005 at <http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/04/08/financial/f100816D42.DTL>

Barkham, Jason, Information Warfare and International Law on the Use of Force,

34 New York Journal of International Law and Polities 57 (2001)

Bassiouni, M Cherif, & Edward M Wise Aut Dedere Aut Judicare. The Duty to Extradite or Prosecute in International Law (Martinus Nijhoff Publishers 1995 – ISBN 0792333497)

Bassiouni, M. Cherif, Universal Jurisdiction for International Crimes: Historical perspectives and contemporary practice, 42 Va.J.Int't L. 81 (2001) niversal Jurisdiction for International Crimes: Historical perspectives and contemporary practice, 42 Virginia Journal of International Law 81 (2001)

Belarus Moves to Limit Online Dating, 14 December 2005, Associated Press <www.forbes.com/work/feeds/ap/2005/12/14/ap2391504.html> (visited December 2005)

Berger, Matt, Yahoo case raises issue of Internet Borders, UpsiteToday, 3 November 2000 <http://www.upsite.com> (visited November 2000)

Bergmank, B., Shortsighted Sentence Policies, Champion May 2006, 30-May Champ 4

Berners-Lee, T. & R. Fielding, Uniform Resource Identifier (URI): Generic Syntax, RFC 3986 (January 2005)

Betænkning nr. 368 af 1964 om behandling af Søsager [Report no. 368 of year 1964 on Maritime Cases]

Betænkning nr. 1052 af 1985 om retternes stedlige kompetence i borgerlige sager [Report no. 1052 of year 1985 on the jurisdiction of courts in civil cases]

Betænkning nr. 435/1996 om pornografi – [White Paper 435 of 1966 on penalty of pornography from the Danish Justice Department's Expert panel]

Betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning - Delbetænkning II afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminallitet - [White Paper 1377 of 1999 on Child Pornography and IT-investigations from the Danish Justice Department's Expert panel on economic and data crimes]

Betænkning 1403/2001 af Maj 2001 - Gennemførelse af forbrugerkøbsdirektivet [White Papere 1403 of 2001 on Amendment pursuant to the E.U. Directive on Consumer purchase] at <www.jm.dk/wimpdoc.asp?page=document&objno=55176> (visited 12. APRIL 2006)

Betænkning nr. 1417/2002 om IT-kriminalitet - [White Paper 1417 of 2002 on IT-Crimes from the Danish Justice Department's Expert panel on economic and data crimes], at <http://www.jm.dk/wimpdoc.asp?page=document&objno=64938> (visited 15

December 2004)

Betænkning nr. 1440/2004 om revision af forbrugeraftaleloven – [White Paper 1440 of 2004 form the Justice department's Expert panel on amendments to the Act on Certain Consumer Agreements], at <http://www.jm.dk/wimpdoc.asp?page=document&objno=71810>

Bing, Jon, Modeller av Rettslige Avveininger med et eksempel fra Norsk Interlegal Rett, Tidsskrift for Rettsvittenskab 1985.395 [Models of legal balancing Process with examples from Norwegian Interlegal Law, Periodical for Legal Science (Oslo)]

Blakesley, Christopher L., Jurisdiction as Legal Protection against Terrorism, 19. Conn. L. Rev. 895

BNA, Japanese government Pushes Choice of Law Protection for Citizens Making Online Deals, BNA's Electronic Commerce & Law, 22 February 2006, Vol. 11 No. 8 page 214, at <http://pubs.bna.com/ip/bna/eip.nsf/eh/a0b2h3g4g3> (visited March 4 2006)

Bogdan, Michael, Komparativ Rättskundskap 91-92 (Norstedts Juridik, Sweden, 1993, 1. Ed. ISBN 91-38-50200-3).

Bogdan, Michael, Svensk internationell privat- og processrätt [Swedish international private- and procedure law] (5. Ed., Norstedts Juridik AB, Stockholm 1999 - 91-38-50115-5)

Børnerådet [Danish Children's Council], Rigtigt og forkert [Right or Wrong] - Report (Copenhagen 2006 – ISBN 87-90946-36-7) at <http://www.boerneraadet.dk/graphics/pdf-filer/andet/Rigtigt%20og%20forkert.pdf> (visited April 2006)

Borum, O.A., Lovkonflikter: lærebog i international privatret [Conflict of law: Textbook on international private law] (4. Ed. 1957 Gads Publishing)

Braden (ed.), Requirements for Internet Hosts – Communication Layers, RFC 1122 (Oct 1989)

Bradner, S. & A. Mankin, The Recommendation for the IP Next Generation Protocol, RFC 1752 (January 1995)

Bradner, The Internet Standards Process - Revision 3, RFC 2026 (October 1996)

Bredsdorff, Magnus & Jakob M. Larsen, Yahoo lukker i Danmark - tabte 66 millioner [Yahoo shut down in Denmark - 66 millions in loss], Computerworld-DK, 22 January 2004 at <http//: www.computerworld.dk-default.asp?Mode=2&ArticleID?22289> (visited 24 January 2004)

Brenner, Susan W. & Bert-Jaap Koops, Approaches to Cyberspace Jurisdiction, 4 Journal of High Technology Law 1 (2004)

Brown, Chip, Fear.com The State of the American Newspaper, American Journalism Review, 21, June 1999, page 51-71. <http://www.ajr.org/Article.asp?id=3230> (visited October 17 2004)

Brownlie, Ian, Principles of Public International Law (6th Edition, Clarendon Press, Oxford – ISBN 0199260710)

Bruhn-Petersen, Frederik, Elektronisk præstation af digitale ydelser [Electronic deliverance of digital output] 22 (Treatise delivered at Copenhagen University April 1999 - <www.jur.ku.dk/it-ret/specialer/bruhn-petersen.pdf >

Buckley, Chris, Internet muck-raker challenges China's Censors, Reuters 17 February 2006 <http://www.prisonplanet.com/articles/february2006/170206censors.htm> (visited Feb 2006

Camarillo, The Internet Assigned Number Authority (IANA) - Header Field Parameter Registry for the Session Initiation Protocol (SIP), RFC 3968 (December 2004)

Canada Customs and Revenue Agency, Report: When Is Non-residents Doing Business In Canada (November 2001) at <http://www.ccra-adrc.gc.ca/tax/technical/ecommerce-e.html> (visited January 2002)

Carlson's online timetable. David Carlon's Virtual World at <http://iml.jou.ufl.edu/carlson/1990s.shtml> (visited October 17 2004)

Carpenter (Ed.), Charter of the Internet Architecture Board, RFC 2850 (May 2000)

Carpenter, B. & C. Jung, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, RFC 2529 (March 1999)

Carpenter, B. & K. Moore & B. Fink, Routing IPv6 over IPv4 – Connecting IPv6 Routing Domains Over the IPv4 Internet, at <http://www.cisco.com/en/US/about/ac123/ac147/ac174/ac197/about_cisco_ipj_archive_article09186a00800c830a.html> (visited October 2005)

Cassese (ed), The Rome Statute of the International Criminal Court: A Commentary (Ed. Antonio Cassese, Oxford University Press 2002 – ISBN 0-19-829862-5)

Cassese, Antonio, International Law (1st Edition, Oxford University Press - ISBN 0-19-829998-2)

Cassese, Antonio, International Criminal Law (Oxford University Press – ISBN 0-19-925911-9)

Catherine Kessedjian, Report on International Jurisdiction and Foreign Judgments in Civil and Commercial Mattes, Hague Conference on Private Interna-

tional Law - Enforcement of Judgments - Prel. Doc. No 7 - Revised Translation of October 1997, at <ftp://ftp.hcch.net/doc /jdgm_pd7.doc> (visited November 2003)

Cavers, David F., Contemporary Conflicts Law in American Perspective, 131 Recueil des Cours 75 (1970-III)

CBC, Cyberstalker sentenced to one year, CBC News, 16 March 2006 <http://www.cbc.ca/story/canada/national/2006/03/16/cyberstalk060316.html> (visited 18 March 2006)

Center for Democracy & Technology, French court rules in favor of Yahoo in Internet free speech case, cdt.org at <http://www.cdt.org/jurisdiction> (visited October 2003)

Cerf to Matt Berger, Yahoo case raises issue of Internet Borders, UpsiteToday, 3 November 2000 <http://www.upsite.com> (visited November 2000)

Cerf, interview on History of the TCP/IP protocol at <http://www.ibiblio.org/pioneers/cerf.html> (visited April 2003)

Cerf, Vinton G. & Robert E Kahn, A Protocol for Packet Network Intercommunication, IEEE Transactions on Communications, May 1979, Vol. Com-22, Number 5 page 637, The IEEE Communications Society

Cerf, Vinton, Experts says France could block most Nazi web sales, Reuters, November 6, 2000

Cerf, Vinton, November 24, 2000 to Top Internet advisor criticizes French Yahoo! Decision, Agence France Press, 2000 WL 24767154 (Westlaw database AGFRP)

Cerf, Vinton, to Arshad Mohammed, Verizon Executive calls for end to Google's "Free Lunch", Washington Post.com, February 7, 2006 at <www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html> (visited February 8, 2006)

Cerf, Vinton, to Lisa Guernsey, Welcome to the Web. Passport, Please?, The New York Times – Technology, March 15, 2001, <http://tech2.nytimes.com/mem/technology/techreview.html?res=9B01E7D71F3AF936A25750C0A9679C8B63> (visited November 27, 2005)

Cerf, Vinton, to Matt Berger, Yahoo case raises issue of Internet borders, UpsiteToday, November 3, 2000 <http://www.upside.com> (visited November 2000)

Chartrand, Mark R., Satellite Communications for the Nonspecialist (Spie Press 2004 – ISBN 0-8194-5185-1)

Cheswick, Bill, to Stefanie Olsen, Geographic tracking raises opportunities, fears,

Cnet News.com, 8 November 2000, at <http://news.com.com/2100-1023_3-248274.html> (visited 14 October 2003)

Chosun, N. Korea's Hackers Rival CIA, Expert Warns, Chosun June 2, 2005 at <http://english.chosun.com/w21data/html/news/200506/200506020014.html> (visited June 2005)

Chosun, N. Korean Military Hackers Conduct War in Cyberspace, Chosun May 27, 2004 at <http://english. chosun.com/w21data/html/news/200405/200405270038.html> (visited June 2005)

Clapham, Christopher, Sovereignty and the Third World State, Political Studies, 47 Pol.Stud. 522, 537 (1999) XLVII

Clinton, William J. & Albert Gore, Jr., A Framework for Global Electronic Commerce (July 4, 1997) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (visited Nov. 21, 1997)

Cohen, Debra R., The Single Publication Rule: One action, not one law, 62 Brooklyn Law Review 921 (1996)

Collins, Matthew, The Law of Defamation and the Internet (Oxford University Press, 2001)

Compaine, Benjamin M., & Douglas Gomery, Who Owns the Media – Competition and Concentration in the Mass Media Industry (Lawrence Erlbaum Associates, Publishers, Third Edition, 2000 – ISBN 0-8058-2935-0)

Conta, A. & S. Deering, Generic Packet Tunneling in IPv6 – Specification, RFC 2473 (December 1998)

Conta, A. & S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) – Specification, RFC 2463 (December 1998)

Convery, Sean & Darrin Miler, IPv6 and IPv4 Threats Comparison and Best-Practice Evaluation (v1.), at <http://www.cisco.com/security_services/ciag/documents/v6-v4-hreats.pdf#search='ipv4%20sean%20convery'> (visited October 21, 2005)

Crampton, Thojmas, Paris Approves Law Aimed at Making iTunes Compatible With Rival Devices, The New York Times, 1 July 2006, at <www.nytimes.com/2006/07/01/business/worldbusiness>

D.J. Harris, Cases and Materials on International Law (5th Edition, Sweet & Maxwell, ISBN 0-421-53470-2Hb)

Daarbak, Torben, [Hacking's a snap in Legoland] ComputerWorld.dk, 16 September 2006 at <http://www.computerworld.dk/art/29810> (visited March 2006)

Dauterman, Walter C., Internet Regulation: Foreign actors and local harms - At the crossroads of pornography, hate speech, and freedom of expression, 28 North Carolina Journal of International Law and Commercial 177 (2002)

de Vries, Henry P. & Andreas F. Lowenfeld, Jurisdiction in Personal Actions – A Comparison of Civil Law Views, 44 Iowa Law Review 306, 332-39 (1959)

de Winter, L. I., Excessive Jurisdiction in Private International Law, 17 International and Comparative Law Quarterly 707 (1968)

Deering, S, & H. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460 (December 1998)

Defense Department Will Require IPv6 Compliance, Says DoD's John Osterholz (Press Release), Market Wire, June 26 2003, at <http://www.findarticles.com/p/articles/mi_pwwi/is_200306/ai_mark1060030660> (visited October 2005)

Desai, Nitin , Annex to Preliminary Report of the WGIG – Introduction, Chairman of the Working Group on Internet Governance (WGIG) in Geneva on 24 February 2005 at <http://www.wgig.org/docs/outline-24-11-04.pdf>

Det Danske Sprog- og Litteraturselskab: Ordbog over det Danske Sprog [The Danish Language and Literature Society: Dictionary on the Danish Language] (2. Ed. Gyldendal Publishing, Copenhagen 1969)

Dommel, Hans-Peter , Routers and Switches, in Handbook of Information Security (Hossein Bidgoli Ed., 2006, Wiley – ISBN0-471-64833-7)

Drozdova, Ekaterina A., Civil Liberties and Security in Cyberspace in Sofaer (ed), The Transnational Dimension of Cyber Crime and Terrorism 58 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5)], also available from <http://www.hoover.org/publications/books/cybercrime.html>. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/183.pdf> (visited May 2006)

Duerst, Internationalized Resource Identifiers (IRIs), RFC 3987 (January 2005)

E.U., Security and Privacy for the Citizen in Post-September 11 Digital Age: A Prospective Overview 30 (European Commission Joint Research Centre July 2003 - EUR 28823 EN) at <http://www.jrc.es/home/publications/publications.cfm?pub=1118> (eur20823en.pdf).

E.U., Special Eurobarometer 60.0, Report from European Opinion Research Group EEIG on comsumer e-commerce (March 2004) at <http://europa.eu.int/comm/consumers/topic/btoc_ecomm.pdf> (visited March

2004)

E-Commerce and Development Report 2003, United Nations, UNCTAD/SDTE/ECB/2003/1 at <http://www.unctad.org/en/docs/sdteecb20031overview_en.pdf >

Edelman, Benjamin, Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users, at <http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf > (visited March 2006)

Edenborough, Michael, Computer Contract/Sale of Goods; Software "Goods" within the Sale of Goods Act 1979, European Intellectual Property Review, 1995, E.I.P.R. 1995, 17(2), D48

Entertainment Law Review, Case Comment: Arnold Schwarzenegger Case not Terminated, 2005, Ent. L.R. 2005, 16(6), 156

Explanatory Report of 8 November 2001 to the Cybercrime at <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (visited December 2005).

Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems, at <http://convention.coe.int/Treaty/en/Reports/Html/189.htm>

Extraterritorial Jurisdiction, 57 Illinois Bar Journal 672 (1969)

Fagan, Kevin, Battling to Preserve Remnants of History, San Francisco Chronicle, 2 November 2000, A17

FBI, A Computer Crime Survey of 2005 at <www.fib.gov/publications.ccs2005.pdf> (visited January 2006)

FBI, IC3 2005 Internet Crime Report, Internet Crime Complaint Center, at <www.ic3.gov> or <www.fbi.gov/publications/ccs2005.pdf> (visited May 2006)

Ferguson, P. & D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827 (May 2000)

Ferguson, P. & D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2267 (January 1998)

First Report on the application of Directive 2000/31/EC, EU Commission, COM(2003) 702 Final of 21. November 2003 at < http://europa.eu.ont/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf>

Fiuczynsky, Marc E., et. al., The Design and Implementation of an IPv6/IPv4 Network Address and Protocol Translator, Section 2.2.1, USENIX Association

1998, <http://www.usenix.org/publications/library/proceedings/usenix98/full_papers/fiuczynski/fiuczynski.pdf#search='Design%20and%20Implementation%20of%20an%20IPv6%2FIPv4%20Network%20Address%20and%20Protocol%20Translator'> (visited October 2005)

Folketings Tidende (F.T.)]Official Journal of Danish Parliament]

Forbrugerombudsmandens Undersøgelse af Danske Internetauktioner [(Danish) Comsumer-Ombudsman's survey on Danish Internet Auctions] of 27 February 2006 <http://www.forbrug.dk/fileadmin/Filer/Markedsf_ring_og_jura/Internetauktioner_-_Rapport_-_konklusioner.pdf> (visited April 2006)

Franklin, Benjamin, Historical Review of Pennsylvania (1759) <http://www.quotationspage.com/quote/1381.html> (visited May 2006)

Friedmann, Wolfgang, The Changing Structure of International Law (Stevens & Sons, 1964)

Gai, Silvano, Internetworking IPv6 with Cisco Routers 26-27, available online at <www.ip6.com/us/book/Chap2.pdf> (last modified June 2004) (visited September 2005)

Geist, Michael, Is there a there there? Toward Greater Certainty for Internet jurisdiction, 661 PLI/Pat 561, 612-615 (July 2001) or <http://aix1.uottawa.ca/~geist/ geistjurisdiction-us.pdf> (visited 2001)

Gibb, Frances, Law lords to rule on internet defamation, Times Online, 26 June 2006 at <http://www.timesonline.co.uk/article/0,,200-2243300,00.html>.

Gilligan, R. & E. Nordmark, Transition Mechanisms for IPv6 Hosts and Routers, RFC 2893 (August 2000)

Goldsmith, Jack L., Against Cyberanarchy, University of Chicago Law Review, 65 U. Chi. L. Rev. 1199 (1988)

Goldsmith, Jack L., The Internet and the Dormant Commerce Clause, 100 Yale Law Journal 785 (March 2001)

Gomard, Civilprocessen [Civil Procedure] (5. Ed. v/Kistrup, GadJura Publishing, Copenhagen 2000 - ISBN 87-619-0204-7)

Gomard, Forholdet mellem Erstatningsregler i og uden for Kontraktsforhold [The relation between rules of damage in and outside contracts] (Gads Publishing, Copenhagen 1958)

Greer, Jennifer, & Donica Mensing, Evolution on Online Newspapers: A longitudinal content analysis, 1997-2003, October 1, 2003, at < http://list.msu.edu/cgi-bin/wa?A2=ind0310a&L=aejmc&D=0&P=1228> (vis-

ited September 2004)

Greve, Vagn, Gitte Høyer, Malene Frese Jensen & Martin Spencer, The Danish Criminal Code & the Danish Corrections Act (2.Ed 2003, DJØF Publishing - ISBN 87-574-0218-3)

Groff, Jeff to Mark Ward, How the web went world wide, BBC NEWS 3 August 2006 at <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/5242252.stm> (visited August 2006)

Guernsey, Lisa, Welcome to the Web. Passport, Please?, The New York Times – Technology, March 15, 2001, <http://tech2.nytimes.com/mem/technology/techreview.html?res=9B01E7D71F3AF936A25750C0A9679C8B63> (visited November 27, 2005)

Gutnick 'delight' on defamation deal, The Australian, November 12, 2004 at <http://www.theaustralian.news.com.au/common/story_page/0,5744,11365187%255E1702,00.html> (visited November 15, 2004)

Hameline, H. Joseph, & William Miles, The Dormant Commerce Clause Meets the Internet, 41-Oct B.B.J. 8 (1997)

Hamilton, Tyler, Battle for the Web, Toronto Star, March 28, 2006 at <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1143499812060&call_pageid=968350072197&StarSource=RSS> (visited March 28, 2006)

Hampton, Philip G., Legal Issues in Cyberspace, 759 PLI/Pat 537, 602-614, Karren M. Shorofsky, The Wide World of Websites: Other current Internet legal topics, SD38 ALI-ABA 451 (1999)

Hansen, Jesper Lau, Nordic Company Law - The Regulation of Public Companies in Denmark, Finland, Iceland, Norway and Sweden, English Translation by Steven Harris (DJØF Publishing, Copenhagen 2003 - ISBN 87-574-0794-0)

Hardy, I. Trotter, The proper Legal Regime for "Cyberspace", 55 University of Pittsburgh Law Review 993 (1994)

Harris, D.J., Law of the European Convention on Human Rights 274 (Butterworths 1995 – ISBN 0-406-25930-5)

Harvard Research in International Law, Draft Convention on Jurisdiction with Respect to Crime, 29 American Journal of International Law (AJIL) 435 (Supp. 1935)

Henkin, Louis, Human Rights and State "Sovereignty", Georgia Journal of International and Comparative LAW 25 Ga. J. Int'l & Comp. L. 31-32 (1995/96)

Henkin, Pugh, Schachter and Smit, International law, Cases and Materials 421

(1980)

Hertz, Ketilbjørn, Værnetingsaftaler i internationale forbrugeraftaler [Forum selection in international consumer agreements], UfR [Journal of Law part B] 1999B.39

Higgins, Rosalyn, Problems & Process – International Law and How We Use it (Clarendon Press, Oxford 1994 – ISBN 0-19-876410-3)

Higgins, Rosalyn, International Law and the Avoidance, Containment and Resolution of Disputes – General Course on Public International Law, 230 Recueil des cours 23 (1991-V)

Higgins, Rosalyn, Respecting Sovereign States and Running a Tight Courtroom, 50 International and Comparative Law Quarterly 121, 122 (2001)(Publisher: British Institute of International and Comparative Law, Oxford University Press)

History - ARPAnet 1957 – 1990, at <http://www.jmusheneaux.com/21bb.htm> (visited December 21, 2005)

Hovey, The Organizations Involved in the IETF Standards Process, RFC 2028 (October 1996)

Hyde, J.E., Decoding the codes: A content analysis of the news coverage of genetic cloning by three online news sites and three national daily newspapers, 1996 though 1998. (Doctoral dissertation, New York University, April 2001) DAI-A 61/10, page 3814.

Information Notice of 1. November 2002, E-Policy and E-Regulatory Framework Development in Transition Economies, U.N. Economic Commission for Europe, <http://www.unece.org/etrades/ict/docs/infonotice.pdf> (visited November 2003)

Information Technology Association of America, Ecommerce Taxation and the Limitations of Geolocation Tools, at <www.itaa.org/taxfinance/docs/geolocationpaper.pdf> (visited March 2006)

International Centre for Missing & Exploited Children, Child Pornography: Model Legislation & Global Review (2006) at <http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf>

IP Version 6 (IPv6) (last updated January 3, 2003) at <http://playground.sun.com/pub/ipng/html/#INTRO> (visited October 2005)

IPng Current Specifications (last updated September 21, 2001) at <http://playground.sun.com/pub/ipng/html/specs/specifications.html#SPEC> (visited October 2005)

ITU and its Activities Related to Internet-Protocol (IP) Networks (Version 1.1,

April 2004) at <http://www.itu.int/osg/spu/ip/itu-and-activities-related-to-ip-networks-version-1.pdf> (visited March 2006)

Jenard Report no. 1 (1979), O.J. C59, 5/3/1979, p. 0001-0065 at <http://aei.pitt.edu/1465/01/commercial_report_jenard_C59_79.pdf> (visited March 2006)

Jenard Report no. 2 (1979), O.J. C59, 5/3/1979, p. 0066-70 at <http://aei.pitt.edu/1466/01/commercial_reports_jenard_protocols_c59_79.pdf > (visited March 2006)

Jenard-Möller Report (1990), O.J. C 198, 28/7/1990, p. 0057-00122 at <http://aei.pitt.edu/1464/01/Commercial_reports_Jenard_OJ_C_189_90.pdf> (visited March 2006)

Johnson, D, C Perkins & J Arkko, Mobility Support in IPv6 draft-ietf-mobileip-ipv6-24.txt (June 30, 2003), at <http://www.merit.edu/internet/documents/ietf/59cdrom/proceedings/I-D/draft-ietf-mobileip-ipv6-24.txt> (visited October 2005)

Johnson, David & David Post, And How Shall the Internet be Governed, Cyberspace Law Institute, at <http://www.cli.org/emdraft.html> (visited December 2005)

Johnson, David R. & David Post, Surveying Law and Borders – The Rise of Law in Cyberspace, 48 Stanford law review 1367 (1996)

Johnson, Phillip, All Wrapped Up? A review of the enforceability of "shrink-wrap" and "Click-wrap" license in the United Kingdom and the United States, European Intellectual Property Review, 2003, E.I.P.R. 2003, 25(2), 98-102

Joyner, Christopher C., & Catherine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, 12 European Journal on International Law 825 (2001)

Jupiter Communications, Portals Emerge as Dominant Source for Online News, New York, Jupiter Communications, December 8, 1998, at <www.jup.com/jupiter/press/releases/1998/1208a.html>

Jurkowitz, Mark, Online News Outlets Catch Their Breath, The Boston Globe online, 19 January 2001, at <http://digitalmass.boston.com/news/daily/01/011901/online_media.html> (visited October 17 2004)

Kanuck, Sean P., Information Warfare: New Challenges for Public International Law, 37 Harvard International Law Journal 272 (1996)

Kardel, Hans, Om værneting efter retsplejelovens §244 [now 243] in UfR [Journal of Law part B] 1984B.61

Karn, P. & P. Metzger, The ESP DES-CBC Transform, RFC 1829 (August 1995)

Karnov Lovsamling [Karnov statute book]

Kaspersen, Henrik W.K., Jurisdiction in the Cyberspace Convention, in Cybercrime and Jurisdiction - A Global Survey (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218)

Kastenholz, F. and C. Partridge, Technical Criteria for Choosing IP: The Next Generation, RFC 1726 (December 1994)

Kennedy, Charles H., An Introduction to International Telecommunications Law (Artech House Inc. 1996 – ISBN 0-890068356)

Kommenteret Retsplejelov [Commentary to the Civil Procedure Code] (DJØF Publishing 2000 - 87-574-6855-9)

Kompella, K., A Traffic Engineering (TE) MIB [Management Information Base], RFC 3970 (January 2005)

Koops (ed.), Cybercrime and Jurisdiction - A Global Survey (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218)

Kuczynski, Alex, Slate Ends Its 10-month Experiment with Subscribtions, The New York Times, February 15, 1999 at <www.nytimes.com/library/tech/99/02/biztech/articles/15slat.html>

Kumar, Aparna ,Online News Frenzy Is Fizzling, Wired News, 12 January, 12 2001 at <http://www.wired.com/news/business/0%2C1367%2C41121%2C00.html> (visited October 17 2004)

Langsted, Lars Bo, Peter Garde & VAgn Greve, Criminal Law Denmark (2 Ed. DJØF Publishing –ISBN 87-574-1057-7)

Lau, J., M. Townsley & I. Goyret (Editors), Layer Two Tunneling Protocol - Version 3 (L2TPv3), RFC 3931 (March 2005)

Law Commission, Defamation and the Internet (UK, December 2002) at <http://www.lawcom.gov.uk/239.htm#1lcr266 (visited October 2003) or <http://www.lawcom.gov.uk/files/defamation2.pdf>

Lee, Roy S., Introduction in The International Criminal Court: The Making of the Rome Statute Issues, Negotiations, Results (Kluwer Law International, 2002 – ISBN 904111212X)

Lee, Soo-jeong, North Korea has 600 computer hackers, South Korea claims, SecurityFocus October 5, 2004 at <www.secutiyfocus.com/news/9649> (visited June 2005)

Lessig, Lawrence, Code and Other Laws of Cyberspace (Basic Books 1999 - ISBN 0-465-03913-8)

Lessig, Lawrence, Legal Issues in Cyberspace: Hazards on the Information Superhighway: Reading the Constitution in Cyberspace, 45 Emory Law Journal 869 (1996)

Lessig, Lawrence, The Future of Ideas – The Fate of the Commons in a connected World (Random House 2001 - ISBN 0-375-50578-4)

Levins, H., Time of Change and challenge (Online Newspapers), Editor & Publisher, 130 (1) page 58

Levkowetz, H. & S. Vaarala, Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519 (May 2003)

Longworth, Elisabeth, The Possibilities for a Legal Framework for Cyberspace, in The International Dimension of Cyberspace Law 30 (Law of Cyberspace Series Vol. 1, Ashgate Publishing 2000 – ISBN 0-7546-2146-4)

Lookofsky, Joseph M, Godsværneting og 'Due Process of Law' [The "Goods-jurisdiction-rule" and 'Due Process of Law'], UfR [Journal of Law part B] 1985B.73

Lovelace, Jack & Kirk Hallahan, Pricing, content and Identity Issues at U.S. Online Newspapers – A Survey of Editors, August 2003, page 1, at <http://lamar.colostate.edu/~pr/onlinelovelace040103.doc> (visited October 9, 2004)

Lukasik, Stephen J., Current and Future Technical Capabilities in The Transnational Dimension of Cyber Crime and Terrorism 125 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5). Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/125.pdf>

Lundgaard, Hans Petter, Gaarders innføring i internasjonal privatrett [Gaarders introduction to international private law] (3 Ed., Universitetsforlaget AS, Oslo, 2000 - ISBN 82-00-45239-5)

Malekian, F., International Criminal Law 40-46 (Borgstrôms Tryckeri AB 1991 – ISBN 91-630-0244-2 & 9)

Malekian, F., Particular Emphasis on the Concept of Crime and Criminal Responsibility 169 (Stockholm 1985)

Mann, Frederich.A., Further Studies in International Law (1990, Clarendon Press, Oxford – ISBN 0198252471)

Mann, Frederich.A., The Doctrine of Jurisdiction in International Law, 111 Recueil Des Cours 1, 46-47 (1964-I)

Map showing the international underwater cables used for international Internet traffic as of the end of 2004 can be found at <http://news.com.com/2300-1033_3-6035611-1.html> (visited May 2006)

Maxmind, GeoIP City Accuracy for Select Countries, at <www.maxmind.com/app/city_accuracy> (visited March 2006)

MaxMind, What are the "A1" Anonymous Proxy entities and How do I tell what the IP address behind a proxy is? at <www.maxmind.com/app/faq>, <www.maxmind.com/app/proxy#open> (visited March 2006)

MaxMind, What are the "A2" Satellite Provider enties? at <www.maxmind.com/app/faq> (visited March 2006)

McCharty, L. Thorne, Reflections on Taxman: An experiment in artificial intelligence and legal reasoning, 90 Harvard Law Review 837

McCulagh, Declan, Government Web sites are keeping an eye on you, CNET News.com 5 January 2006 <http://news.com.com/2100-1028_3-6018702.html> (visited January 2006)

McCullagh, Declan, Bush pushes for Cybercrime treaty, News.Com 18 November 2005 at <http://news.com.com/Bush+pushes+for+cybercrime+treaty/2100-1028_3-5108854.html> (visited November 2005)

McCullagh, Declan, First 'cybercrime' treaty advances in Senate, CNET News.Com 26 July 2005 at <http://news.com.com/2100-7348_3-5805561.html> and <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QE1> (visited May 2006)

McCullagh, Declan, Fuzzy logic behind Bush's Cybercrime treaty, News.Com 28 November 2005 at <http://news.com.com/2010_1071_3-5969719.html> (visited November 2005)

McCullah, Declan, Data thief gets eight years, News.Com 24 February 2006 at <http://news.com.com/2100-7348_3-6042290.html> (visited March 2006)

Merryman, John H, The Civil Law Tradition: Europe, Latin America, and East Asia 547 (The Michie Company 1994 – ISBN 1-55834-180-3)

Metzger, P. & W. Simpson, IP Authentication using Keyed MD5, RFC 1828 (August 1995)

Meyer, Eric, More Get Caught Up in the Web, American Journalism Review, 6 February 2001, <http://newslink.org/emcol8.html> (visited October 17 2004)

Miller, Mark A., Internet Technologies Handbook (Wiley-Interscience, 2004 – ISBN 0-471-48050-9)

Minnesota Attorney General making a "Warning to all Internet users and provid-

ers" at <www.ag.state.mn.U.S./home/consumer/consumernews/OnlineScams/ggpress .html> (visited March 15, 1999)

Munch, Mogens, Udlæg i fordringer på en skyldner i udlandet [Execution into debt of a person outside Denmark], UfR [Journal of Law part B] 1966B.217

Nagpal, Rohas, Tools and techniques of cybercrime, Asian School of Cyber Laws at <www.asianlaws.org/cyberlaw/library/cc/cc_tt.htm>.

Nanda, P. & David K. Pansius, Litigation of International Disputes in U.S. Courts §1:31, LOID S 1:31 (August 2005)

National Conference of Commissioners, Handbook of the National Conference of Commissioners on Uniform State Laws

Nielsen, Peter Arnt, International privat- og procesret [International private- and procedure law](DJØF Publishing, Copenhagen 1997 -87-574-7630-6)

Nørarger-Nielsen & Teilgaard, Købelovskommentaren (2. Ed. 1993, Gads Publishing - ISBN 87-12-01567-9)

Nordmark, E. & R. Gilligan, Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213 (October 2005)

North, Peter, & J.J. Fawcett, Cheshire and North's Private International Law (3rd Ed. 1999 – ISBN 0-406-90596-7)

OECD, Report on The Development of Broadband Access in Rural and Remote Areas of 10 May 2004 - Working Party on Telecommunication and Information Services Policies, (OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, DSTI/ICCP/TISP(2003)7/FINAL) at <www.oecd.org/dataoecd/24/ ??/31718094.pdf> (visited February 2005).

Olsen, Stefanie, Geographic tracking raises opportunities, fears, Cnet News.com, 8 November 2000, at <http://news.com.com/2100-1023_3-248274.html> (visited 14 October 2003)

Oppenheim's International Law (London and New York: Longman 9th Ed., paperback edition 1996 – ISBN 0582302455)

Oppenheim's International Law Vol. II on Disputes, War and Neutrality (7th Ed. Edited by H. Lauterpacht, Longmans 1952)

Øren, Joakim S.T., International Jurisdiction and Consumer Contracts – Section 4 of the Brussels Jurisdiction Regulation ((Complex 5/04, Norwegian Research Center for Computers and Law, Oslo University 2004, ISBN 82-7226-082-4)

Østergaard, Kim, Elektronisk Handel og International Proces- og Privatret (DJØF Publishing, Copenhagen 2003 - ISBN 87-874-0969-2)

Out-Law, Tool can resurrect deleted cookies, Out-Law 5 April 2005 at <http://www.out-law.com/page-5502> (visited May 2006)

OUT-Law.com, Ex-Yahoo CEO's Nazi auction acquittal upheld in France, OUT-Law.com, April 7, 2005 (visited April 7, 2005).

Out-Law.com, French court acquits Yahoo! of criminal charges for Nazi sales, Out-Law.com, February 12, 2003 at <http://www.out-law.com/php/page.php?page_id= frenchcourtacquits104505511&area=news> (visited February 19, 2003)

Out-Law.com, Lords restrict terror website censorship plans, Out-Law.com 3 February 2006 at <www.out-law.com/page-6602> (visited February 2006).

Oxman, Bernard H., Arrest Warrant of 11 April 2000, 96 Am.J.Int'l L. 677

Patwari, Neal, et al., Locating the Nodes, IEEE Signal Processing Magazine page 66, no. 54, July 2005, also at <www-personal.engin.umich.edu/~npatwari/localizationMag.pdf> (visited March 2006)

Paust, Jordan J., International Law as Law of the United States (Carolina Academic Press 1996 – ISBN 0890898626)

Perkins (Ed.), IP Mobility Support, RFC 2002 (October 1996)

Philip, Allan, American-Danish Private International Law 24 in Bilateral Studies in Private International Law no. 7 (Ed. Arthur Nussbaum, Oceana Publications, New York 1957)

Philip, Allan, Dansk International Privat- og procesret 81 [Danish International Private- and Procedural law] (3 ed. DJØF Publishing, Copenhagen 1976 - ISBN 87-574-1962-0)

Philip, Allan, Domskonventionen: EF-IP II, Værneting-Tvangsfuldbyrdelse af fremmede retsafgørelser (1986) s. 144 (DJØF Publishing, Copenhagen 1986)

Plonka, Embedding Globally-Routable Internet Addresses Considered Harmful, RFC 4085 (June 2005)

Postel, The TCP Maximum Segment Size and Related Topics, RFC 879 (Nov 1983)

Postel, Internet Protocol, RFC 791 (1981)

Princeton Principles at <www.princeton.edu/~lapa/unive_jur.pdf>

Putham, Tonya L. & David D. Elliott, International Responses to Cyber Crime in The Transnational Dimension of Cyber Crime and Terrorism 58 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5)] also available from

<http://www.hoover.org/publications/books/cybercrime.html>. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/35.pdf > (visited May 2006)

Randall, Kenneth C., Universal Jurisdiction under International Law, 66 Texas Law Review. 785 (1988)

Rapport de Consultation in the French Yahoo case, at <http://www.law-links.ch/archiv00.html file rapportyahoo-6nov00.zip> (visited May 2003)

Raz, Uri, How do I find the geographical location of a host, given its IP address?, at <http://www. private.org.il/IP2geo.html> (visited June 2003)

Redegørelse om auktioner på Internettet [Whitepaper on auctions on the Internet] of 14 March 2006 from the Justice Department (Doc. KLH40242 – j.nr. 205-709-0017) at <www.jm.dk/image.asp?page=image&objno=75160> (visited April 2006)

Reidenberg, Joel, Technology and Internet Jurisdiction, 153 University of Pennsylvania Law Review 1951 (June 2005)

Rekhter, CIDR and Classful Routing, RFC 1817 (August 1995)

Report of the meeting of the inter-sessional open-ended intergovernmental group of experts on the elaboration of a preliminary draft of a possible comprehensive international convention against organized transnational crime, U.N. Doc. E/CN.15/1998/5 of 18 February 1998 at <www.uncjin.org/Documents/7comm/5e.pdf> (visited 11 May 2006)

Reporters Without Borders, Enemies of the Internet (Reporters Sans Frontieres, 2001) <http://www.rferl.org/nca/special/enemies.html> (visited January 22 2003)

Reporters Without Borders, The Internet under Surveillance - Obstacles to the Free Flow of Information online, 2003 Report (Reporters Sans Frontieres - ISBN 2-90-8830-88-4) <www.rsf.org/IMG/pdf /doc-22236.pfd> (visited September 2003)

Request for Comments (RFC) published by the Internet Architecture Board, at <http://www.ietf.org/rfc.html>

Restatement (First) of Conflict of Laws (American Law Institute)

Restatement (Third) of Foreign Relation Law (American Law Institute)

Restatement Tort (Second) (American Law Institute)

Reuters, Dutch site linking to MP3 files loses court case, Reuters, 19 June 2006 at <http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2006-06-19T105335Z_01_L19632414_RTRUKOC_0_US-INTERNET-MUSIC.xml> (visited July 2006)

Reuters, French courts aquits ex-Yahoo chief over Nazi sites, LycosNews, February 11, 2003 at <http://news.lycosasia.com /sgen/> New York Times, February 11, 2003, <http://www.nytimes.com/reuters /technology/tech-crime-france-yahoo.html> & News.Com, February 11, 2003 at <http://news.com.com/2100-1023-984148.html> (all visited 18 February 2003)

Reynolds et. al., Internet Official Protocol Standards, RFC 3300 (November 2002)

Reynolds, J. & J. Postel, The Request for Comments Reference Guide, RFC 1000 (August 1987)

RFC Editor et al., 30 Years of RFCs, RFC 2555 (April 1999)

Rosenne, Shabtai, The Perplexities of Modern International Law 450 (2004, Martinus Nijhoff Publishers – ISBN 9004136924)

Ross, Teemu, et al., A Probabilistic Approach to WLAN User Location Estimation, International Journal of Wireless Information Networks, p. 155, Vol. 9, no. 3, July 2002, also at <www.cs.helsinki.fi/u/ttonteri/pub/ijwin02.pdf> (visited March 2006)

Rothkrug, Lionel, Defamation: Uniform Single Publication Act, 44 California Law Review147 and footnote 5 (1956)

Safferling, Christoph J.M., Towards an International Criminal Procedure 321 (Oxford University Press 2001 – ISBN 0-19-926450-3)

Savola, P. & C. Patel, Security Considerations for 6to4, RFC 3964 (December 2004)

Savola, Pekka, Migration and Co-existence of IPv4 and IPv6 in Residential Networks, CSC/FUNET, at <http://staff.csc.fi/~psavola/residential.html> (visited October 2005)

Scheeres, Julia, Europeans Outlaw Net Hate Speech, Wired News 9 November 2002 at <http://www.wired.com/news/business/0,1367,56294,00.html> (visited November 26, 2005)

Schjølberg, Stein, A Global Survey of Cybercrime Laws with translation into English is available at Cybercrimelaw.net (a global information clearinghouse on cybercrime law, edited by Council of Europe expert on cybercrime & Chief Judge Stein Schjølberg, Norway) at <http://www.cybercrimelaw.net/laws/survey.html >

Schjølberg, Stein, and Amanda M. Hubbard, Computer Crime and Intellectual Property Division, U.S. Justice Department, Harmonizing National Legal Approaches on Cybercrime 18, WSIS Thematic Meeting on Cybersecurity June 2005, Doc: CYB/04

<http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf> (visited May 2006)

Schjølberg, Stein, Law Comes to Cyberspace: A presentation at the 11th UN Criminal Congress, 18-25 April 2005, Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime, <http://www.cybercrimelaw.net/documents/UN_Bangkok_05.htm> (visited May 2006)

Schlosser Report (1978), O.J. C59, 5/3/1979, p. 0071-0151 at <http://aei.pitt.edu/1467/01/commercial_reports_schlosser_C_59_79.pdf> (visited March 2006)

Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Columbia Journal of Transnational Law 885 (1999)

Schwarzenegger Case not Terminated, Case comment in Entertainment Law Review 2005, Ent. L.R. 2005, 16(6), 156

Scotsman, Judge: Extradite 'Super-hacker' to US, The Scotsman 11 May 2006 <http://thescotsman.scotsman.com/international.cfm?id=704082006> (visited May 2006)

Security Threat Management Report 2005 (Sophus) at <www.securitymanagement.com/library/trojans_sophos0206.pdf> (visited May 2006)

Shannon, Victoria , A Compromise of Sorts on Internet Control, The New York Times, November 16, 2005 at <www.nytimes.com/2005/11/16/technology/16net.html> (visited 16 November 2005)

Shaw, Malcolm N., International Law (4th Edition, Cambridge University Press – ISBN 0521576679)

Shearer, I.A., Starke's International Law (11th Edition, Butterworth – ISBN 0406016232)

Shen, N. & H. Smit, Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels, RFC 3906 (October 2004)

Shorofsky, Karren M., Advertising and Promotions on the Internet, 563 Practising Law Institute (Pli/Pat) 659.

Siesby, Erik, Godsværneting og sikkerhedsstillelse [Goods-jurisdiction-rule and security], Juristen 1974.532

Siesby, Erik, Godsværnetinget og forum rei sitæ [The goods-jurisdiction rule and

forum rei sitæ], Juristen 1974.84

Siesby, Erik, Udlændinges værneting og udlandsdanskeres [Foreigners jurisdiction and Danes abroad], UfR [Journal of Law part B] 1980B.381

Silicon Valley.com, French Appeals court says Yahoo not liable for Nazi gear auctions, Silicon Valley.com, April 6 2005 at <www.siliconvalley.com/mldsiliconvalley/news/editorial/11326488>

SiliconValley.com, 21-year-old hacker sentenced to nearly 5 years in prison, SiliconValley.com 9 may 2006 at <www.siliconvalley.com/mid/siliconvalley/news/editorial/14537874.htm> (visited May 2006)

Singel, Ryan, Giving New Meaning to 'Spyware', Wired News 12 July 2005 at <http://www.wired.com/news/privacy/0,1848,68167,00.html>

Sluizer, Suzanne, to Paul Feste, End of the road for STMP?, CNET News.com, 1 August 2003 at <http://news.com.com/End+of+the+road+for+SMTP/2100-1038_3_5058610.html> (visited March 2005)

Socolofsky, T. & C. Kale, A TCP/IP Tutorial, RFC 1180 (Jan. 1991)

Sofaer (ed), The Transnational Dimension of Cyber Crime and Terrorism 58 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5)], also available from <http://www.hoover.org/publications/books/cybercrime.html> (visited May 2006)

Sofaer, Abraham D., Toward an international Convention on Cyber Security in Sofaer (ed), The Transnational Dimension of Cyber Crime and Terrorism 58 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5)], also available from <http://www.hoover.org/publications/books/cybercrime.html>. Also available at <www-hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf > (visited May 2006)

Sophus, Security Threat Management Report 2005 at <www.securitymanagement.com/library/trojans_sophos0206.pdf> (visited May 2006)

Spang-Hanssen, Henrik, Afslutning på Yahoo-sagen [The End of the Yahoo case], Lov & Data page 33-35, [Law and Data Journal 1/2006] (Published in Scandinavia, ISSN 0800-7853)

Spang-Hanssen, Henrik, Californiske Yahoo! Inc. contra Frankrig: en international tvist på Internettet [Califonian Yahoo! Inc contra France: A international dispute on the Internet], Lov & Data page 18-22, [Law and Data Journal]

4/2001] (Published in Scandinavia, ISSN 0800-7853)

Spang-Hanssen, Henrik, Cybercrime and Jurisdiction in Denmark, in Cybercrime and Jurisdiction - A Global Survey 170-172 (Ed. Bert-Jaap Koops & and Susan W. Brenner, 2006 T.M.C. Asser Press, The Hague – ISBN 9067042218)

Spang-Hanssen, Henrik, Cyberspace & International Law on Jurisdiction - Possibilities of Dividing Cyberspace into Jurisdictions with help of Filters and Firewall Software (DJØF Publishing, Copenhagen 2004 – 87-547-0890-1 – US Congress Library 2004441311)

Spang-Hanssen, Henrik, Cyberspace Jurisdiction in the U.S.: The International Dimension of Due Process (Complex 5/01, Norwegian Research Center for Computers and Law, Oslo University 2001 - ISBN 82-7226-046-8 – US Congress Library 2003450386), also free downloading from research website <www.geocities.com/hssph>

Spang-Hanssen, Henrik, Filtering and blocking of websites content and legislation on the Internet - including the Yahoo case at <www.geocities.com/hssph> under Articles (Translation of article Filterblokerng af websiders indhold og lovgivning af Internettet – herunder Yahoo-sagen on page 321-328 in Kritisk Juss [Norwegian Law Journal "Critical Law"] No. 3-4/2001, Norway, ISSN 0804-7375)

Spang-Hanssen, Henrik, Hollywood puts 3 Baltic countries into a Second Class of E.U. or Hollywood does not recognize E.U.'s single market from May First 2004 at <www.geocities.com/hssph/articles>.

Spang-Hanssen, Henrik, Indtrængen ("deep linking") i andres databaser [Deep linking in others databases] Lov & Data page 1-3, [Law and Data Journal] 4/2001] (Published in Scandinavia, ISSN 0800-7853)

Spang-Hanssen, Henrik, "Net defamation" in Australian IT, August 29, 2001 at <http://australianit.news.com.au/common/story-PAGE/0,3811,%202783041%255E506,00.html> (visited September 2001)

Spang-Hanssen, Henrik, Opdatering i sagen Yahoo! Inc. mod LICRA [An update on the case between Yahoo! Inc and LICRA], Lov & Data page 7, [Law and Data Journal] 2/2005] (Published in Scandinavia, ISSN 0800-7853)

Spang-Hanssen, Henrik, Peer-to-Peer – Grokster, Lov & Data page 18-24, [Law and Data Journal] 1/2006] (Published in Scandinavia, ISSN 0800-7853)

Spang-Hanssen, Henrik, The earthly chaos in websites - question of jurisdiction and net-censorship (Translation of article The jordiske kaos over websider – jurisdiktionsspørgsmål og netcensur, Kritisk Juss page 63-67 [Norwegian Law Journal "Critical Law"], No. 1-2/2001, Norway, ISSN 0804-7375)

Spang-Hanssen, Henrik, Who should govern telecommunications on the public international computer networks, Chapter to "The U.N. and the Future of International Law" in Honor of Honorable Ronald St. J. MacDonald - Edited by Bertrand Ramcharan (Publisher: Martinus Nijhoff (upcoming 2006))

Spleth, P., Retspleje i borgerlige sager - Udlændinges værneting [Administration of justice in civil cases - Foreigners Jurisdiction], UfR [Journal of Law part B] 1964B.264

Stallings, William, High-Speed Networks and Internets: Performance and Quality of Service 5 (2. Ed. 2002, Prentice Hall – ISBN 0-13-032221-0)

Stallings, William, IPv6: The New Internet Protocol at <http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stalings> (visited February 2005)

Statement of Principles applicable to the Formation of General Customary International Law as amended at the 2000 London conference (International Law Association) at <http//:www.ila-hq/pdf/CustomaryLaw.pdf>

Stein, Allan R., Personal Jurisdiction and the Internet: Seeing Due Process through the Lens of Regulatory Precision, 98 Northwestern University Law Review 411 (2004)

Steinhardt, Barry to Declan McCullagh, Bush pushes for Cybercrime treaty, News.Com 18 November 2005 at <http://news.com.com/Bush+pushes+for+cybercrime+treaty/2100-1028_3-5108854.html> (visited November 2005)

Stephens, Richard, The Legal Principles Governing the Supply of Computer Systems: Part 1, Computer and Telecommunications Law Review, 1998, C.T.L.R. 1998, 4(2), 27

Steptoe, A guidance on Internet Security at <www.steptoe.com/publications/365b.pdf> (visited May 2006)

Sullivan, Carl, Papers Run Nearly Half Of Top 20 News Sites, Editor & Publisher, September 12, 2002 at <http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1698470> (visited October 7, 2004)

Sussman, Douglas, Censor dot Gov: the internet and press freedom 2 (2000) <http://www.freedomhouse.org/pfs2000/sussman.htniJ>

Svantesson, Dan, Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet, 23 J. Marshall J. Computer & Info. L. 101 (Fall 2004)

Tapper, Colin, The "Oxford Experiments", Prediction of Juridicial Decisions, Computers and The Law 232-251 (London 1973)

Terdiman, Daniel, Hacking's a snap in Legoland, Cnet News.com, 15 September 2005 at<http://news.com.com/Hackings+a+snap+in+Legoland/2100-1046_3-5865751.html>

Thaler, IP Tunnel MIB, RFC 4087 June 2005)

The Domain Name System: A case study of the significance of norms to Internet Governance, Harvard Law Faculty, 112 Harvard Law Review 1657 (1999)

The International Dimensions of Cyberspace Law (UNESCO's series on Law of Cyberspace series, UNESCO Publishing, 2000 – ISBN 92-3-103752-8)

Thornburgh, Dick, & Herbert S. Lin, A Global Internet" in Youth, Pornography, and the Internet section 11.2 (Dick Thornburgh & Herbert S. Lin, eds., National Academy Press, 2002), at <http://search.nap.edu/html/youth_internet> or <http://www.nap.edu>.

Thoumyre, Lionel, La Cour d'appel de Paris se déclare compétente pour examiner la responsabilité de l'ex-PDG de Yahoo! Inc., Juriscom.net March 17 2004, at <http://www.juriscom.net/actu/visu.php?ID=477> (visited August 28 2004)

Townsley, Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update, RFC 3438 (December 2002)

Trzaskowski, Jan, Legal Risk Management in Electronic Commerce – managing the risk of cross-border law enforcement (Ex Tuto Publishing, 2005 – ISBN 87-991018-0-7)

Tunis Agenda for the U.N. World Summit on the Information Society, reprinted in Outcome Documents (International Telecommunication Union, December 2005) at <www.itu.int/wsis/promotional/outcome.pdf> (visited July 2006)

Tunkin, G.I., Theory of International Law 244 (London 1974)

Turk, Configuring BGP to Block Denial-of-Service Attacks, RFC 3882 (September 2004)

U.N. Economic Commission for Europe, Information Notice of 1. November 2002, E-Policy and E-Regulatory Framework Development in Transition Economies, <http://www.unece.org/etrades/ict/docs/infonotice.pdf> (visited November 2003)

U.S. Principles on the Internet's Domain Name and Addressing System at <www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm > (visited July 5, 2005)

United Nations Treaties and Principles on Outer Space 22 (2002 - ISBN 92-1-100900-6) at <http://www.unoosa.org/pdf/publications/STSPACE11E.pdf>

Universal Jurisdiction in Europe since 1990 for war crimes, crimes against humanity, torture and genocide (Redress, 30 June 1999) at <www.redress.org>

van Blarcum, Internet Hate Speech: The European Framework and the Emerging American Haven, 62 Washington and Lee Law Review 781 (2005)

von Hebel, Herman, Elements of Crimes in The International Criminal Court: Elements of Crimes and Rules of Procedure and Evidence (Ed. Roy S. Lee, Transnational Publishers 2001 – ISBN 157105-209-7)

von Mehren, Arthur T., & Donald T. Trautman, Recognition of Foreign Adjudications: A Survey and a suggested Approach, 81 Harvard Law Review 1601 (1968)

Walsh, Jennifer E., Tough for Whom?: How prosecutors and judges use their discretion to promote justices under the California Three-strikes law (Henry Salvatory Center 2004) at <http://salvatori.claremontmckenna.edu/publications/pdf/Walshmonograph.pdf> (visited May 2006)

Ward, Mark, How the web went world wide, BBC NEWS 3 August 2006 at <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/5242252.stm> (visited August 2006)

Weitzenböck, Emily M., Electronic Agents and the Formation of Contracts, International Journal of Law and Information Technology, Vol. 9 No. 3, 204-234, (Oxford University Press 2001) <http://www3.oup.co.uk/inttec> (visited July 2003)

Weitzenböck, Emily M., Good Faith and Fair Dealing in Contracts Formed and Performed by Electronic Agents, in Chapter 9 of YULEX 2005 (Institutt for rettsinformatik, Oslo University 2005 – ISBN 82-7226-094-8)

Werlauff, Erik, Civil Procedure - Denmark (1 Ed. 2001, DJØF Publishing - ISBN 87-574-0496-8)

Werlauff's Kommenterede Aktieselskabslov (2. Ed. DJØF Publishing 2002 - ISBN 87-574-0589-1)

WGIG, Legal aspects of electronic commerce of 26 August 2003 (A/CN.9/WG.IV/WP.103) <http://www.unicitral.org /en-index.htm> (acn9-528-e.pdf & wp-103-e.pdf)

WGIG, U.N. Report of the Working Group IV on Electronic Commerce of 19 May 2003 (A/CN.9/528)

Wilson, George D. et. al, A Proposal for an International Convention on Cyber Crime and Terrorism (Draft by George D. Wilson, Abraham D. Sofaer and Gregory D. Grove, Center for International Security and Cooperation (CISAC), Hoover Institution) <http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf> (visited May 2006), re-

printed in The Transnational Dimension of Cyber Crime and Terrorism 58 (Eds. A. Sofaer and S. Goodman, Hoover Institution Press 2001 – ISBN 0-8179-9982-5), also available from <http://www.hoover.org/publications/books/cybercrime.html> (visited May 2006)

WIPO, The Management of Internet names and Addresses: Intellectual Property Issues - Final Report of the WIPO Internet Domain Name Process 30 April 1999 at <http://arbiter.wipo.int/processes/process1/report/finalreport.html> (visited May 2006).

Wired, Report: U.S. Spies on Everyone, Wired News 11 May 2006 at <www.wired.com/news/wireservice/1,70878-0.html> (visited May 2006

Witkin, California Criminal Law Vol. 3, 456 (3rd Ed. 2000)

World Factbook of Criminal Justice Systems at <http://www.ojp.usdoj.gov/bjs/abstract/wfcj.htm> (visited May 2006).

World Intellectual Property Organization, Intellectual Property on the Internet: A survey of Issues (December 2002 – Doc. WIPO/Int/02) at <http://ecommerce.wipo.int/survey/pdf/survey.pdf> (visited 2003)

Wright, Tom, EU Tries to Unblock Internet Impasse, The New York Times, September 30, 2005 at <www.nytimes.com/iht/2005/09/30/business/IHT-30net.html> (visited October 14, 2005)

WSIS Outcome documents (International Telecommunication Union, December 2005) at <www.itu.int/wsis/promotional/outcome.pdf> (visited July 2006)

Yokoyama, Dennis T., You can't always use the Zippo code: The fallacy of a uniform theory of Internet Personal Jurisdiction, 54 DePaul Law Review 1147 (2005)

Zeller, Tom, Cyberthieves Silently Copy Your Passwords as You Type, The New York Times 27 February 2006 at <http://www.nytimes.com/2006/02/27/technology/27hack.html> (visited May 2006)

Zero-Knowledge Systems' application "Websecure" at <http://www.freedom.net/products/websecure/howitworks.html> (visited 14 October 2003)

Zhao, H., ITU and Internet governance, 15 December 2004, ITU Council Working Group on the World Summit on the Information Society Geneva 13-14 December 2004, WG-WSIS-7/6 Rev 1 at <www.wgig.org/working-papers.html> (visited March 2005)

Zweigert, K. & H.Kotz, Introduction to Comparative Law 277 (Clarendon Press,

Oxford 1998, 3rd Edition – Translation by Tony Wier – ISBN 0-19-826859-9)

12. Cases

To find a Danish Case from a normal Danish citation (see further Appendix 10, Abbrivations), go to the end of this appendix 12 and find the name of the parties. Thereafter, go to the following caselaw-list and find the book-page(s) where the case is dealt with.

Cases

1st Mover Aps (Denmark) v. Direct Hedge S.A. (Switzerland), UfR 2002.1370 Ø (Eastern Appeal Court 7 March 2002) 379, 391
A Munck v. Alkan, Heumann & Co. (Germany), UfR 1924.350 SH (The Maritime and Commercial Court in Copenhagen, 13 February 1924) 416
A v Italy, Human Rights Committee (HRC) Doc A/43/40, 242 332
A v. Baan Nordic A/S (tidligere Beologic A/S), UfR 2001.697 Ø (Easter Appeal Court 26. November 1999) 385
A/S Frederik Fiedler v. Firmaet E. Zoubir (Algeria), UfR 1925.453 SH (The Maritime and Commercial Court in Copenhagen, 31 March 1925) 416
A/S Jølving v. firmaet Wallengreen & Co (Sweden), UfR 1954.609 SH (The Maritime and Commercial Court in Copenhagen, 12 March 1954) 416
A/S N. Foss Electric v. John Shields (England), UfR 1979.616 SH (The Maritime and Commercial Court in Copenhagen 14 March 1979) 394
A/S Svendborg Kasein v. Etablissements Freddy Baines (Netherlands), UfR 1955.1079 SH (The Maritime and Commercial Court in Copenhagen 8 July 1955) 407, 412
A/S Svendborg Kasein v. Freddy Baines S.A., UfR 1956.657 H (Supreme Court of Denmark, 7 May 1956) 412
Aage Thorning-Christensen v. Ella Hartvig Henriksen, UfR 1945.393 Ø (Easter Appeal Court, 19 December 1944) 414, 418
ACLU v. Reno, 217 F.3d 162 (3rd Cir. 2000) 199, 314, 315
Advent Systems Ltd. v. Unisys Corp., 925 F.2d 670 (3rd Cir 1991) 390
Ahlstrom Osakeyhtio v Commission of the European Communities (E.C.J. C89/85 1988), [1988] 4 C.M.L.R. 901, 1988 E.C.R. 5193 98
Ahlstrom Osakeyhtio v Commission of the European Communities (E.C.J. C89/85 1993), 1993 E.C.R I-1307 98
Aktieselskabet Havnemøllen (Aalborg) v. Firma Je-Ba v/J. Jensen (Glostrup), VLT 1957.292 (Western Appeal Court 15. June 1957) 393
Alfa-Bank v. S, UfR 2000.1635 Ø (Easter Appeal Court 6 April 2000) 379
Alfred Leopold (Norge) v. Carl Davidsen, UfR 1940.454 H (Supreme Court of Denmark 3

April 1940) 395, 396
Allan Haugsted v. Firma Maretec A.G. (Switzerland), UfR 1990.475 V (Western Appeal Court 1 March 1990) 411
American Banana Company v. United Fruit Company, 213 U.S. 347 (1909) 324
American Booksellers Foundation v. Dean, 342 F.3d 96 (2nd Cir. Aug. 2003) 215
American Civil Liberties Union v. Johnson, 194 F.3d 1149 (10th Cir. 1999) 215
American Civil Liberties Union v. Reno, 31 F.Supp.2d 473 (E.D.Pa. 1999) 12, 110, 130, 190
American Civil Liberties Union v. Reno, 929 F.Supp 824 (E.D.Pa. 1996) 12, 110, 187
American Eyewear, Inc. v. Peeper's Sunglasses and Accessories, Inc., 106 F.Supp.2d 895 (N.D.Tex. 2000) 184
American Libraries Association v. Pataki, 969 F.Supp. 160 (S.D.N.Y. 1997) 215
American Library Association, Inc. v. United States, 201 F.Supp.2d 401 (E.D.Pa. May 2002) 226
Andelsanstalten "Vort Land" (Dansk Syge- og Ulykkesforsikringsselskab) v. Edv. Ph. Mackeprang, UfR 1913.721 (Landsover- and Hof- and Stadsretsdomme, 27 January 1913) 397
Anna Richardson v. Arnold Schwarzenegger, Sean Walsh and Sheryl Main [2004] EWHC 2422 (High Court, Queens Bench Division, October 29 2004 – case no. HQ04X01371) 33, 141, 241, 247, 257, 330
Anselmi v. The Denver Post, Inc., 552 F.2d 316 (10th Cir. 1977) 231
Aquino v. Electriciti Inc., 26 Med.L.Rptr. 1032 (Cal. Superior, Sep. 1997) 227
Asahi Metal Industry Co., Ltd. v. Superior Court of California, 480 U.S. 102 (U.S. (Cal) 1987) 177
Ashcroft v. American Civil Liberties Union, 124 S.Ct. 2783 (US, June 29 2004) 279
Ashcroft v. American Civil Liberties Union, 535 U.S. 564, 122 S.Ct. 1700 (U.S. May 2002) 165
ASX 265 A/S v. Ulrik Flening, UfR 1975.428 H (Supreme Court of Denmark 24 March 1975) 376
Attorney General of Israel v. Eichmann, 36 I.L.R. 277 (Isr. S. Ct., 29 May 1962) 123
Attorney General of Israel v. Eichmann, 36 I.L.R. 5 (Isr. D.C., Jerusalem, 12 Dec. 1961) 123
Bainbridge v. Turner, 311 F.3d 1104 (11th Cir. 2002) 214
Bancroft & Masters, Inc. v. Augusta Nat'l Inc., 223 F.3d 1082 (9th Cir. 2000) 133, 187, 266
Bangoura v. Washington Post, see Cheickh Bangoura 141
Barcelona Traction, Light, and Power Co, Limited (Belgium v. Spain) (Second Phase) of February 5, 1970, 1970 I.C.J. 3 ..... 11, 41, 100
Barcelona.com, Inc. (U.S.) v. Excelentisimo Ayuntamiento de Barcelona (City Council of Barcelona, Spain), 330 Fed 617 (4th Cir. 2003) 117
Barrett v. Catacombs Press, 44 F.Supp.2d 717 (E.D. Pa. 1999) 186, 194

Bauherrengemeinschaft (Germany) v. Konkursboet Bent Iversen, UfR 1987.14 H (Supreme Court of Denmark 13 November 1986) 413
Bejle Gardiner I/S under konkurs v. Eilermark A.G. (Germany), UfR 1978.575 V (Western Appeal Court 14 March 1978) 377
Bensusan Restaurant Corp., v. King, 937 F.Supp. 295 (S.D.N.Y.1996) 180, 186
Bensusan Restaurant Corp., v. King,126 F.3d 25 (2nd Cir. 1997) 180, 186
Bent Bjerregaard Thomsens konkursbo v. Astramaris Schifahrtskontor G.m.b.H. (Germany), UfR 1973.206 V ((Western Appeal Court, 13 November 1972) 414
Bent Manholm v. Andalucia International Real Estate, UfR 1982.266 Ø (Easter Appeal Court 27 November 1981) 383, 387
Berezosky v. Michaels & Berezosky v. Forbes, [2000] E.M.L.R. 643 ..... 141, 240, 398
Berezovsky v. Forbes Inc., [1999] I.L.Pr. 358 para. 37, 1998 WL 1043805, [1999] E.M.L.R. 278, (English Court of Appeal, 1998) 141, 240
Beta Computers (Europe) Ltd. v. Adobe Systems (Europe) Ltd., [1996] F.S.R. 367 (Court of Session - Outer House (Scotland) 390
Bird v. Parsons, 289 F.3d 865 (6th Cir. (Ohio) May 2002) 120, 133, 178
Bjørn Bartig (Sweden) v. Den Danske Landmandsbank A/S, UfR 1968.384 H (Supreme Court of Denmark, 1 April 1968) 416
Blackburn v. Walker Oriental Rug Galleries, Inc., 999 F.Supp. 636 (E.D.Pa. 1998) 181, 190
Bochan v. La Fontaine, 68 F.Supp.2d 692 (E.D.Va. 1999) 186, 195
Bonnier Media Limited v. Greg Lloyd Smith, [2002] E.T.M.R 86, 2003 S.C. 36 (Scottish Outer House, July 2002 - A1334/02) 374
Brein v. Techno Design (Dutch Appeal Court, June 2006) 356
British Telecommunication Plc v. Prodigy Communications Corp., 217 F.Supp.2d 399 (S.D.N.Y., Aug. 2002) 377
Brunswick A.G. v. C.E. Jensen, UfR 1964.228 H (Supreme Court of Denmark 14 February 1964) 410, 417, 418
Burnham v. Superior Court of California, 495 U.S. 604 (US 1990) 115
Cable News Network v. CNNews.com, 56 Fed.Appx. 599 (2003) 117
Calder v. Jones, 465 U.S. 783 (US 1984) 120, 178, 187, 194, 246, 251, 372, 397
Campbell v. American International Group, Inc. 976 P.2d 1102 (Okla. Civ. App. 1999) 184, 187
Canal Digital Danmark A/S v. Hans Magnus Carlsson, UfR 2001.2186 Ø (Easter Appeal Court 26 June 2001) 290, 397
Capstan Shipping Ltd. ApS v. ScanPly International Wood Products Ltd. (Hong Kong), UfR 1988.579 SH (The Maritime and Commercial Court in Copenhagen, 24 February 1988) 413, 418
Carafano v. Metrosplash.com, Inc., 207 F.Supp.2d 1055 (C.D.Cal. 2002) 227
Carrot Bunch Co, Inc. v. Computer Friends, Inc., 218 F.Supp.2d 820 (N.D.Tex. Aug.

2002)..... 119
Case against Karadzic before International Criminal Tribunal for the former Yugoslavia 329
Case against Milosevic before International Criminal Tribunal for the former Yugoslavia 329
Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) of June 27, 1986, 1986 I.C.J. 14..... 285
Case concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium) of 14 February 2002, 2002 ICJ 121..... 100, 122, 275
CEAG Sicherheitstechnik GmbH v. Eksportkreditfonden EKF, UfR 2001.1529 H (Supreme Court of Denmark 19 April 2001) 377
Centros Ltd (United Kingdom) v. Erhvervs- og Selskabsstyrelsen (Denmark [Trade- and Companies Board]), E.J.C. case C-212/97 of 9 March 1999..... 386
Cheickh Bangoura v. Washington Post, 2004 CarswellOnt 340 (Ontario Superior Court of Justice, 27 January 2004)..... 141, 142, 237, 238, 247
Cheickh Bangoura v. Washington Post, 2005 CarswellOnt 4343 (Ontario court of Appeal, September 16 2005) 141, 142, 237, 238, 239, 247, 257
Cheickh Bangoura v. Washington Post, 2006 CarswellOnt 932 (Supreme Court of Canada, February 16, 2006 – Docket 21203)..... 143, 239
Chiaphua Components Ltd. v. West Bend Comp., 95 F.Supp.2d 505 (E.D.Va. 2000) ... 167, 189
Christian Science v. Nolan, 259 F.3d 209 (4th Cir. July 2001) 133
Citigroup Inc. v. City Holding Co., 97 F.Supp.2d 549 (S.D.N.Y. 2000) 188
Coastal Video Communications, Corp. v. Staywell Corp., 59 F.Supp.2d 562 (E.D.Va. 1999)..... 193
Colt Studio, Inc. v. Badpuppy Enterprise, 75 F.Supp.2d 1104 (C.D.Cal. 1999)..... 184
Commonwealth of Virginia v. Jeremy Jaynes (Circuit Court of Virginia, Loudoun County - Judge Thomas D. Horne, November 2004 - Criminal Nos 15885, 15886, 16121) .. 288
CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996)..... 184, 375, 392
Con-Mec A/S v. Fournais Handels- & Ingeniørfirma A/S, UfR 1998.728 SH (The Maritime and Commercial Court in Copenhagen 18 February 1997)..... 376
CoolSavings.com, Inc. v. IQ.Commerce Corp., 53 F.Supp.2d 1000 (N.D.Ill. 1999) 191
Coprosider S.p.A. (Italy) v. Vølund Energiteknik A/S, UfR 1985.904 H (Supreme Court of Denmark 29 August 1985)..... 393
Core-Vent Corp. v. Nobel Industries AB, 11 F.3d 1482 (9th Cir. 1993) 162, 372
Cubby, Inc. v. CompuServe, Inc, 776 F.Supp. 135 (S.D.N.Y. 1991)..... 226
Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997)..... 120, 123, 135, 178
Cyberspace Communications, Inc. v. Engler, 238 F.3d 420 (6th Cir. 2000) 215
Cyberspace Communications, Inc. v. Engler, 55 F.Supp.2d 737 (E.D. Mich. 1999) 215
Dagesse v. Plant Hotel NV, 113 F.Supp.2d 211 (D.N.H. 2000) 188, 190

Damstahl A/S v. A.T.I. s.r.l. (Italy), UfR 2001.1039 H (Supreme Court of Denmark 15 February 2001) 389
Danske Dagblades Forening v. Newsbooster, UfR 2003.1063 SH (The Maritime and Commercial Court in Copenhagen 19 February 20003) 358
Dansk-spansk vinimport D.S.V. A/S under konkurs v. Anselm Mayrs dødsbo (Switzerland), UfR 1985.709 Ø (Easter Appeal Court 11 March 1985) 381
Decker v. Circus Circus Hotel, 49 F.Supp.2d 743 (D.N.J. 1999) 187, 190, 195
Denenberg v. Ruder, 2006 WL 379614 at *4 (D. Nebraska, Feb. 2006) 120
Denver Area Educational Telecommunications Consortium, Inc. v FCC, 518 U.S. 727 (U.S. 1996) 15, 104, 155, 196, 342
Desktop Technologies, Inc. v. Colorworks Reproduction & Design, Inc., 1999 WL 98572 (E.D.Pa. 1999) 187
Digital Equipment Corp. v AltaVista Technology, Inc. 960 F.Supp. 456 (D.Mass. 1997) 123, 184
Direktoratet for Københavns skattevæsen v. Poul Ingvar Steen, UfR 1964.224 H (Supreme Court of Denmark, 10 February 1964) 420
Doe v. AOL, 783 S.2d 1010 (Supreme Court of Florida, 2001) 227
Don King v. Lennox Lewis, Lion Promotions, L.L.C. & Judd Burstein, [2004] EWCA Civ1329 (Court of Appeal (Civil Division),19. October 2004) 240, 241
Don King v. Lennox Lewis, Lion Promotions, L.L.C. & Judd Burstein, [2004] EWHC 168, 2004 WL 62126 (High Court of Justice Queen's Bench Division 6 February 2004) 240, 247, 248, 257, 398
Dow Corning International Ltd. (Belgium) v. Dansk Tyggegummifabrik A/S, UfR 1986.922 H (Supreme Court of Denmark 28 October 1986) 394
Dow Jones v. Gutnick,[2002] HCA 56, 42 I.L.M. 41, 2002 WL 31743880, 210 CLR 575, 194 ALR 433, 77 ALJR 255, [2003] AIPC 91-842 (High Court of Australia, 10 December 2002 - No. M3/2002) 142, 217, 244, 245
Dow Jones v. Harrods, 346 F.3d 357 (2nd Cir. Oct 2003) 245, 247
Dring v. Sullivan, 423 F.Supp.2d 540 (D. Md., Mar 30, 2006) 288
Duke of Brunswick v. Harmer, 117 Eng. Rep. 75, 14 Q.B. 185 (Q.B. 1849) (Eng. Queens Bench, 1849) 227, 251, 418
DVD Copy Control Association v. Andrew Brunner, Jon Lech Johansen, Masters of Reversed Engineering (MoRE), et. al., 10 Cal.Rptr.3d 185, 116 Cal.App.4th 241 (Cal.Ct.App.6.Dist., February 27, 2004) 360
Easthaven Ltd. V. Nutrisystem.com Inc., 2001 CarswellOnt 2878 (Ontario Superior Court, No. 00-CV-202854, August 2001) 118, 164, 373
Edberg v. Neogen Corp., 171 F.Supp.2d 104 (D.Conn. 1998) 123
Electronic Broking Services, Ltd. England v. E-Business Solutions & Services, 285 F.Supp.2d 686 (D.Md, Sept. 30, 2003) 396
Erik Fiehn v. A/B Wivefilm (Sweden), UfR 1947.187 Ø (Easter Appeal Court 16 October

1946)..... 395
Erik Mølgaard Petersen v. Helge Otto Jørgensen, UfR 1991.779 Ø (Easter Appeal Court 3 June 1991)..... 388
ESAB Group, Inc. v. Centricut, LLC, 34 F.Supp.2d 323 (D.S.C., 1999)..... 186, 191
Eti-Tuber A/S v. Firma Theodor Klass (Germany), UfR 1968.336 V (Western Appeal Court 18. December 1967)..... 409, 418
EU Commission v. Kingdom of Spain (E.C.J. C-358/01 of 6 November 2003)..... 212
Euromarket Design, Inc. v. Crate & Barrel Ltd., 96 F.Supp.2d 824 (N.D.Ill., 2000)..... 197
European Parliament v Council of the European Union & Commission of the European Communities, 2006 E.C.R… (E.C.J. C-317/04 and C-318/04, 30 May 2006)..... 340
Ewing v. California, 538 U.S. 11 (US Supreme Court March 2003)..... 334
Fausto v Hickman, 2003 WL 21439215 (N.D. Cal., 9 June 2003 – No. C00-4617 MMC(PR))..... 334
Felixstowe Dock & Railway Co. (England) v. Investorgruppen Danmark K/S and A/S Det Østasiatiske Kompagni, UfR 1990.597 H (Supreme Court of Denmark 14 June 1990)..... 376
Ferguson v. Friendfinders, Inc., 94 Cal.App.4th 1255 (California Court of Appeal, 1st Dist, Jan 2002)..... 288
Filomeno Mario Miraglia, 2005 E.C.R I-02009, O.J. C 132 , 28/05/2005 P. 0010 – 0011 (ECJ (Fifth Chamber), 10 March 2005 - Case C-469/03)..... 333
Firma Electronic v. Konkursboet Stenløse Plastic, UfR 1978.876 H (Supreme Court of Denmark 2 October 1978)..... 377, 413
Firma Karl O. Helm v. H.A. Hagbarth A/S, UfR 1962.247 H (The Maritime and Commercial Court in Copenhagen 11 October 1961)..... 376
Firmaet Harald Kjær & Co v. Rederiet Nielsen & Thorden O/Y (Helsinki, Finland), Forsikrings-Aktieselskabet Urania v. "Madrid, Sociedad anonima de reaguros" (Spain), UfR 1926.84 H (Supreme Court of Denmark 22 December 1925)..... 412
Firmaet M Friis-Møller & Co v. Firmaet Tandberg & Wigeland (Norway), UfR 1930.402 Ø (Easter Appeal Court 31 January 1930)..... 410
Firth v. State of New York, 12 A.D.3d 907, 785 N.Y.2d 755 (N.Y.AD.3 Dept., 18 November 2004)..... 255
Firth v. State of New York, 306 A.D.2d 666, 761 N.Y.S.2d 361 (N.Y.A.D. 3.Dept. 2003)..... 236, 255
Firth v. State of New York, 4 N.Y.3d 709, 830 N.E.2d 1145, 797 N.Y.S.2d 816 (N.Y. May 2005)..... 255
Firth v. State of New York, 98 N.Y.2d 365, 775 N.E.2d 463, 747 N.Y.S.2d 69, 30 Media L. Rep. 2085 (N.Y. 2002)..... 234, 235, 253, 254, 255
Flensburger Volksbank A.G. v. Firmaet Jacob Sørensen & Co, UfR 1926.17 H (Supreme Court of Denmark 16 November 1925)..... 407
Flesher v. University of Evansville (Supreme Court of Indiana, No. 82S04-0008-CV-477,

October 2001) 149, 201
Forsikringsselskabet Nye Danske Lloyd v. Stausberg ingenieurbau G.m.b.H. (Germany), Scan-Report A/S v. Forum Annonsbyrå AB (Sverige), UfR 1972.1031 SH (The Maritime and Commercial Court in Copenhagen 13 July 1972) 393
Fulton v. Faulkner, 516 US 325 (U.S. 1996) 214
Gator.com Corp. V. L.L.Bean, Inc., 2001 WL 1528393 (N.D.Cal. 21 November 2001). 134
Gator.com Corp. v. L.L.Bean, Inc., 341 F.3d 1072 (9th Cir. Sep. 2003) ..131, 134, 135, 136, 137, 138, 366
Gator.com Corp. V. L.L.Bean, Inc., 366 F.3d 789 (9th Cir. April 29, 2004) 134
Gator.com Corp. V. L.L.Bean, Inc., 398 F.3d 1125 (9th Cir. Feb. 15, 2005) 134, 138
Gentry v. eBay, Inc., 121 Cal.Rptr.2d 703, 2002 WL 1371153 (Cal.App.4 Dist., June 2002) 182
Gorman v. Ameritrade Holding Corp., 293 F.3d 506 (D.C.Cir. June 2002) 120, 131, 132, 178, 189
Göta hovrätt (Sweden) v. Bodil Lindqvist, E.C.J. C-101/01 (E.C.J., 6 November 2003) 385
Grutkowski v. Steamboat Lake Guides & Outfitters, Inc., 1998 WL 962042 (E.D.Pa. 1998) 187
Gunnar Quistgaard Vemb v. L. Egebjerg, UfR 1957.613 V (Western Appeal Court 26 February 1957) 398
Gutnick v. Dow Jones & Co, Inc, [2001] VSC 305, 2001 WL 966287 (Supreme Court of Victoria (Australia) Aug, 2001 - NO. 7763 of 2000) 243
H.H.Andersen Konfektion Aps v. Textilwerke Ganahl A.G. (Austria), UfR 1997.565 SH (The Maritime and Commercial Court in Copenhagen, 24 March 1977) 414
Handelsfirmaet Vacuum Oil Co A/S v. R Mithassel, UfR 1921.908 SH (The Maritime and Commercial Court in Copenhagen, 26 August 1921) 410, 415
Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214 (2002) 117
Hartford Fire Insurance Co v. California, 509 U.S. 764 (US 1993) 118
Hasbro, Inc. v. Clue Computing, Inc., 994 F.Supp 34 (D.Mass. 1997) 123, 204
Healthcare Alliance Inc. v. Healthgrades.com, Inc., 123 S.Ct. 1909 (US April 28, 2003, No. 02-1250) 119, 372
Healthcare Alliance Inc. v. Healthgrades.com, Inc., 50 Fed.Appx. 339, 2002 WL 31246123 (9th Cir. 2002) 119, 372
Healy v. Beer Institute, 491 U.S. 324 (U.S. 1989) 215
Hearst Corp. v. Goldberger, 1997 WL 97097 (S.D.N.Y. 1997) 123
Helicopteros Nationale de Colombia, S.A. v. Hall, 466 U.S. 408, 414-416 (U.S. 1984) . 118
Hockerson-Halberstadt, Inc. v. Costco Wholesale Corp., 2000 WL 726888 (E.D.La., 2000) 195
Hockerson-Halberstadt, Inc. v. Propet USA, Inc, 62 Fed.Appx 322, 2003 WL 1795641 (Fed Cir. April 2003) 133
Home A/S v. OFIR a-s (The Maritime and Commercial Court in Copenhagen, 24 February

2006 - docket No. V-108-99) at <http://www.domstol.dk/media/-300011/files/v010899.pdf>.....208, 359
Horace Holman Group Ltd. v. Sherwood International Group Ltd., 2000 WL 491372 (High Court of Justice in Queen's Bench's Division Technology and Construction Court, April 2000 - No. 1999-TCC-NO.129).....390
Hotelkette "Maritim" (Germany) v. Hotel Maritime (Copenhagen) (Landgerecht Hamburg, 16. Chamber 3. August 2001- Az: 416 O 294/00).....373
Hotelkette "Maritim" (Germany) v. Hotel Maritime (Copenhagen)(Hanseatisches Oberlandsgericht Hamburg - 3. Zivilsenat, 2. May 2002 - Az: 3 U 312/01).....373
Hurley v. Cancun Play Oasis International Hotels, 1999 WL 718556 (E.D.Pa. 1999)....190, 195
Hüseyin Gözütok and Klaus Brügge, O;J. C 083 , 05/04/2003 P. 0005 – 0005, 2003 E.C.R. I-01345 (ECJ, 11 February 2003 - C-187/01 and C-385/01).....334
HY Cite Corporation v. Badbusinessbureau.com, L.L.C., 297 F.Supp.2d 1154 (W.D. Wisconsin, Jan. 8, 2004).....374, 397
I.H. Nordgren (Sweden) v. Rederiaktiebolaget "Högmarsåo" (Sweden), UfR 1932.645 Ø (Easter Appeal Court 11 March 1932).....393, 394
Industriaktiebolaget EUROC v. Inger Topsøe & Swegon AB (Sweden), UfR 1987.690 H (Supreme Court of Denmark 15 July 1987).....413
Inset Systems, Inc. v. Instruction Set, 937 F.Supp. 161 (D.Conn. 1996).....184, 187
Intel Corp. v. Hamidi, 30 Cal.4th 1342, 71 P.3d 296, 1 Cal.Rptr.3d 32 (Supreme Court of California, Jun 30, 2003).....289
Inter System Transport Ltd. (England) v. Hans Erik Harbos konkursbo, UfR 1974.548 H (Supreme Court of Denmark, 28 May 1974).....417
International Shoe v. State of Washington, 326 U.S. 310 (US 1945).....115, 130, 162, 251
International Star Registry of Illinois v. Bowman-Haight Ventures, Inc., 1999 WL 300285 (N.D.Ill. May 6, 1999 - No. 98 C 6823).....184, 187
Irvin B. Gold v. Chevron Petroleum Company of Denmark, UfR 1989.969 Ø (Easter Appeal Court 20 June 1989).....383
Islandsk Kompagni A/S v. Oskar Halldorsson, UfR 1927.516 SH (The Maritime and Commercial Court in Copenhagen, 4 February 1927).....408
Jacobellis v. Ohio, 378 U.S. 184 (US 1964).....329
Jason O'Grady v. Superior Court of Santa Clara County (Apple Computer), 44 Cal.Rptr.3d 72, 2006 WL 1452685 (Cal.App. 6 Dist., May 26, 2006 - No. H028579).....223, 316
JB Oxford Holdings, Inc. v. Net Trade Inc., 76 F.Supp.2d 1363 (S.D.Fla. 1999).....187
Jewish Defense Organization, Inc. v. The Superior Court of Los Angeles County, 72 Cal.App.4th 1045 (Cal.App. 2 Dist., 1999).....198
Johann H. Anthon A/S v. Bogesundsmaskiner AB (Sverige), UfR 1971.512 V (Western Appeal Court 3 February 1971).....411
Jørgen Jakob Hempel v. I.C.H. Industrial and Commercial Holding A/S, UfR 1982.441 H

(Supreme Court of Denmark 25 March 1982) 376
Jurisdiction of the Courts of Danzig Case, P.C.I.J., Rep. Ser. B., no. 15 (1928) 329
K v. Fogedretten i X-by, UfR 2003.136 V (Western Appeal Court 7 March 2003)..... 419
Kanarek v. Bugliosi, 108 Cal.App.3d 327, 166 Cal.Rptr. 526, 6 Media L. Rep. 1864 (Cal.App.2.Dist. 1980)..... 233, 254
Keeton v. Hustler Magazine, Inc., 465 U.S. 770 (U.S. 1984)..... 204
Kilchem Adriatic of 25/6/1993 A/S v. Office National de l'Huile (Tunisia), UfR 1996.950 SH (The Maritime and Commercial Court in Copenhagen 22. April 1996) 412
Klapmølle Dambrug (Spain) v. B.S. Forellen, UfR 1990.408 V (Western Appeal Court 27. February 1990)..... 388
Klaus Brügge, O;J. C 083 , 05/04/2003 P. 0005 – 0005, 2003 E.C.R. I-01345 (ECJ, 11 February 2003 - C-187/01 and C-385/01) 334
Københavns ny Tømmer-Handel A/S v. Rederiet for m/s "Alma", UfR 1951.1117 SH (The Maritime and Commercial Court in Copenhagen 27 April 1951) 415
Købmand Bernhard Petersen (Iceland) v. Købmand P.J. Torfason (Iceland), UfR 1920.626 Ø (Easter Appeal Court, 10 May 1920)..... 420
Kokkinakis v. Greece, [1993] ECHR 20 (European Court of Human Rights, 25 May 1993 No 14307/88) 335
Kreativt Center A/S v. Karen Margrethe Reiff, UfR 1984.324 V (Western Appeal Court 23 January 1984)..... 380
Kubik v. Route 252, Inc., 762 A.2d 1119 (Pa. Super. 2000) 181
Kulko v. California Superior Ct., 436 U.S. 84 (U.S. (Cal), 1978)..... 192
L'Association Union des Etudiants Juifs de France & La Ligue Contre Le Racisme et L'Antisémitisme v. La Société Yahoo! Inc. & La Société Yahoo France (Tribunal de Grande Instance de Paris, No. RG 00/05308 & 00/05309)..... 32
Lakin v. Prudential Securities, Inc., 348 F.3d 704 (8th Cir. Nov. 2003)...131, 133, 138, 139, 140
Landsbanki Islands Lögfrændingadeild v. Akzo Nobel Chemicals B.V. (the Netherlands), UfR 2002.290 H (Supreme Court of Denmark 6 November 2001) 376
Lauritzen v. Larsen, 345 U.S. 571 (U.S. 1953)..... 113
Le Ministère Public, Association Amicale des Déportés d'Auschwitz et de S Camps de Haute Silesie and M.R.A.P. Mouvement contre le racisme et Pour L'amitié entre les Peuples v. Société Yahoo! Inc et Timothy Koogle (Cour D'Appel de Paris - 11ème Chambre, section A – Dossier No 03/01520)..... 263
Lee Teck Chee v. Merrill Lynch International Bank Ltd., [1998] 4 CLJ 188 (High Court Lalaya, Kuala Lumpur (Malaysia), 26 February 1998 - Civil No. S2-23-51-1997) 237
Leo R. Hertzberg et. al. v. Finland, Communication No. R.14/61, U.N. Doc. Supp. No. 40 (A/37/40) at 161 (1982), Communication No. 61/1979 (Fifteenth session), CCPR/C/15/D/61/1979 (Jurisprudence)..... 158
Leopold Henri Van Esbroeck,2006 E.C.R 00000 (ECJ (Second Chamber), 9 March 2006 -

Case C-436/04) 333
Levine (United States District Court, E.D. Arkansas. (Little Rock) Feb 2006) 353
Lewis v Reader's Digest Ass., Inc. 512 P.2d 702 (Mont. 1973) 231
Lockyer v. Andrade, 538 U.S. 63 (US Supreme Court March 2003) 334
Lofton v. Turbine Design, Inc., 100 F.Supp.2d 404 (N.D.Miss. 2000) 194
Los Angeles Time v. Free Republic, 1999 WL 33644483 (C.D.Cal. Nov. 8, 1999 – CV 98-7840-MMM) 208
Loutchansky v Times Newspapers Ltd (No 2) [2001] EMLR 876 242
Loutchansky v. The Times Newspapers Ltd., [2001] EWCA Civ 1805, [2002] 1 All ER 652 (England and Wales Court of Appeal, 5th December, 2001) 240
Lund-Hansen Advokatvirksomhed ApS v. Benedikte Moeskær, UfR 2002.1676 Ø (Easter Appeal Court 15 April 2002) 381
Maritz, Inc. v. Cybergold, Inc., 947 F.Supp. 1328 (E.D.Mo. 1996) 184
MaryCLE v. First Choice Internet, Inc., 166 Md.App. 481, 890 A.2d 818 (Court of Special Appeals of Maryland, Jan. 26, 2006) 288
Mattel, Inc. v. Barbie-Club.com, 310 F.3d 293 (2002) 117
McBee v. Delica, 2003 WL 1872907, 2003 U.S. Dist. LEXIS 6123 (D. Maine, April 14, 2003) 119
McBee v. Delica, 2003 WL 21553820 (D. Maine, July 9, 203) 119
McMaster-Carr Supply Company v. Supply Depot, Inc., 1999 WL 417352 (N.D.Ill. 1999) 192
McNiel v Verisign & ICANN, 2005 WL 741939 (9th Cir., April 2005) 30
Merrion v. Jicarilla Apache Tribe, 455 U.S. 130 (US 1982) 214
Metcalf v. Lawson, 2002 WL 1369639 (N.H. June 2002) 181
Metro-Goldwyn-Mayer Studios v. Grokster, 243 F.Supp.2d 1073 (C.D.Cal Jan. 2003) .. 132
Meyers v. Bennett Law Offices, 238 F.3d 1068 (9th Cir. (Nev), 2001) 187
Millennium Enterprises, Inc. v. Millennium Music LP, 33 F.Supp.2d 907 (D.Or.1999) 132, 167, 188, 192, 371, 406
Miller v. State of California, 413 U.S. 15 (U.S. (Cal), 1973) 199, 314
Mills Creek Coal & Coke Co, v. Public Service Com., 84 W.Va. 662, 100 S.E. 557, 7 A.L.R. 1081 (W.Va. 1919) 215
Mink v. AAAA Development LLC, 190 F.3d 333 (5th Cir. (Tex) 120, 131, 138, 178
Mohammed Hussein al Amoudi v. (1) Jean Charles Brisard & (2) JCB Consulting International Sarl, [2006] EWHC 1062 (England and Wales High Court (Queen's Bench Division – Justice Gray) 242, 243
Molnlycke Health Care AB v. Dumex Medical Surgical Products Ltd, 64 F.Supp.2d 448 (E.D.Pa. 1999) 132, 189
Morgan Crucible Company Plc. v. A.B. Svejseteknik ApS., UfR 2001.432 SH (The Maritime and Commercial Court in Copenhagen 21 November 2001) 396
National Football League v. Miller d/b/a NFL Today, 2000 WL 335566 (S.D.N.Y. 2000)

.....186
Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883 (6th Cir. (Mich) Mar. 2002) ..120, 178
Niels Mousten Vestergaard v. European Homes B.V. & European Construction B.V. (Netherlands), UfR 1977.395 Ø (Easter Appeal Court 22 December 1977).....413
Nissan Motor Co., Ltd. v. Nissan Computer Corporation, 246 F.3d 675 (9th Cir. (Cal), 2000).....192
Nissan Motor Co., Ltd. v. Nissan Computer Corporation, 89 F.Supp.2d 1154 (C.D.Cal., 2000).....192
Nordisk Fjer A/S v. Firma Samuel Motzen (Romania) UfR 1942.660 SH (The Maritime and Commercial Court in Copenhagen, 27 March 1942).....412
Northern Light Technology v. Northern Light Club, 97 F.Supp.2d 96 (D.Mass. 2000) ..184
Ole Bruun ApS v. Schmict O.H.G. Lederfabrik und Kunststoffwerke (Austria), UfR 1978.863 Ø (Easter Appeal Court, 19 June 1978) 416
OMI Holdings, Inc. v. Royal Insurance Company of Canada 149 F.3d 1086 (10th Cir. 1998).....163
OMI Industries, Inc, v. Kiekert AG, 155 F.3d 254 (3rd Cir. 1998).....163
Opel Austria GmbH v. Council of the European Union (E.C.J. T-115/94 1997), 1997 E.C.R. II-39.....98
Oregon Waste Systems, Inc. v. Department of Environmental Quality of The State of Oregon, 511 U.S. 93 (U.S. 1994) 213
Origin Instruments Corp. v. Adaptive Computer Systems, Inc., 1999 WL 76794 (N.D.Tex. 1999).....191, 195
Orla Stenhøj v. Eksportkreditrådet, UfR 1982.220 V (Western Appeal Court, 23 November 1981) 381
Outokumpu Engineering Enterprises, Inc. v. Kvaener Enviropower, Inc. 685 A.2d 724 (Del. 1996) 163
Pakistans Ambassade v. Shah Travel, UfR 1999.939 H (Supreme Court of Denmark 5 March 1999).....408
Panavision v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) 118, 120
Pebble Beach Company v. Caddy, 2006 WL 1897091, --- F.3d --- (9th Cir. July 2006) ..190
Perkins v. Benquet Consol. Min. co, 342 U.S. 437 (US 1952).....119
Pike v. Bruce Church, Inc., 397 U.S. 137 (U.S. 1970) 213
PIL-Pak A/S v. Crownson Fabrics Ltd., UfR 2002.424 SH (The Maritime and Commercial Court in Copenhagen 8. November 2001).....392
Playboy Enterprise, Inc. V. Chuckleberry Publication, Inc. (Tattilo), 939 F.Supp 1032 (S.D.N.Y. 1996) 123
Porsche Cars North America, Inc. v. Porsche.Net, 302 F.3d 248 (2002).....117
Poul Erik Andersen v. William Mønster, UfR 1938.1094 Ø (Easter Appeal Court 12 August 1938).....394

Poul Erik Bøjden v. Bikuben Girobank A/S, UfR 1997.707 H (Supreme Court of Denmark 11. March 1997) 390
Precision Laboratory Plastic, Inc. v. Micro Test, Inc., 981 P.2d 454 (Wash. Ct. App.Div.2, 1999) 192
Prince Plc v. Prince Sports Group Inc., [1998] F.S.R. 21, 1997 WL 1104934 (English High Court of Justice (Chancery Div,) July 1997) 163
Pro-C Ltd. v. Computer City, Inc. 2001 CarswellOnt 3115, 149 O.A.C. 190, 55 O.R. (3d) 577 (Eng.), 55 O.R. (3d) 583 (Fr.), 205 D.L.R. (4th) 568, 14 C.P.R. (4th) 441 (Ontario Court of Appeal for - No. C34719, Sep. 2001) 186
ProCD, Inc v Zeidenberg, 86 F 3d 1447 (U.S. Appeals Court for 7th Cir 1996) 375, 392
Procecution v. Jon Lech Johansen (Oslo First Instance court (criminal division), 7. January 2003 - Docket 02-507 M/94) 360
Procecution v. Jon Lech Johansen, LB-2003-00731 (Borgating Appellate Court, 22 December 2003 - Docket 03-00731 M/02) 360
Procureur de La Republique, Association Amicale des Déportés d'Auschwitz et de S Camps de Haute Silesie and M.R.A.P. Mouvement contre le racisme et Pour L'amitié entre les Peuples v. Société Yahoo! Inc et Timothy Koogle (Tribunal de Grande Instance de Paris, 17eme Chambre - No d'affaire: 0104305259) 261, 262
Prosecutor v. Erik Georg Gotthards et al., UfR 1940.156 Ø (Court of Appeals for Eastern District, 21 October 1939 – Doc. I 251/1039) 344
Prosecutor v. T, UfR 1978.1003 Ø (Courts of Appeals for Eastern District, 1978) 351
Prosecutor v. T, UfR 1987.216 Ø (Courts of Appeals for Eastern District, 1987) 352
Prosecutor v. T, UfR 1990.70 H (Supreme Court of Denmark, 24 November 1989) 345
Prosecutor v. T, UfR 1996.1538 Ø (Courts of Appeals for Eastern District, 1996) 355
Prosecutor v. T, UfR 1996.356 Ø (Court of Appeals for Eastern District, 22 November 1995 – Doc. S-1948-95) 345
Prosecutor v. T, UfR 1996.979 Ø (Courts of Appeals for Eastern District, 1996) 354
Prosecutor v. T, UfR 1999.177 V (Court of Appeals for Western District, 1999) 356, 361
Prosecutor v. T, UfR 2000.1181 Ø (Courts of Appeals for Eastern District, 2000) 351
Prosecutor v. T, UfR 2000.1450 Ø (Courts of Appeals for Eastern District, 2000) 354
Prosecutor v. T, UfR 2001.2573 Ø (Courts of Appeals for Eastern District, 5. September 2001) 361
Provident Nat. Bank v. California Federal Sav. & Loan Ass'n., 819 F.2d 434 (3rd Cir. 1987) 119
Quokka Sport, Inc. v. Cup International Ltd., 99 F.Supp.2d 1105 (N.D.Cal. 1999) 184
R. v. 800-Flowers Trade Mark, [2002] F.S.R. 12, 2001 WL, 2001] EWCA Civ 721483071 (English Court of Appeal, May 2001) 166
R. v. Keegstra, CarswellAlta 192, 77 Alta. L.R. (2d) 193, 1 C.R. (4th) 129, [1991] 2 W.W.R. 1, 61 C.C.C. (3d) 1, 117 N.R. 1, 114 A.R. 81, 3 C.R.R. (2d) 193, [1990] 3 S.C.R. 697 (Supreme Court of Canada, December 1990) 312

Ramirez v. Castro, 365 F.3d 755 (9th Circuit April 2004) 334
Rano v. Sipa Press, Inc., 987 F.2d 580 (9th Cir. 1993)..... 162
Reno v. American Civil Liberties Union, 521 U.S. 844, 877 (US, 1977) 154, 172, 182, 193, 199, 315, 369
Revell v. Lidov, 317 F.3d 467 (5th Cir. Dec 2002) 131, 133
Rigsadvokaten (US: Attorney General) v. Teleselskabet [tele-company] Debitel, UfR 2005.3446 H (Danish Supreme Court, 22 September 2005) 288, 349, 353
Robbins v. Yutopian Enterprises, Inc., 202 F.Supp.2d 426 (D.Ma. May 2002) 189, 193
Romero v. Holiday Inn, 1998 WL 961384 (E.D.Pa., 1998) 190
Romero v. International Terminal Operating Co, 358 US. 354 (US 1959)..... 113
S v Germany, European Commission on Human Rights (ECommHR) 13 December 1983 Appl. No. 8945/80, 39 DR, 43 332
S. Bjerregaard & Sønner Fiskeeksport A/S under konkurs v. Gulf Fish Trading Ltd. (Holland), UfR 1999.88 H (Supreme Court of Denmark 19. October 1998)..... 413
S.S. Lotus (France v. Turkey) 1927 P.C.I.J. (Ser. A) No. 10 10, 41, 99, 147, 160, 274, 275, 278, 317
Sabroe Refrigeration A/S and Sabro Refrigeration Inc. (USA) v. Lars C. Matthiesen, UfR 1995.898 H (Supreme Court of Denmark – 28 August 1995)..... 376
Sabroe Refrigeration A/S and Sabro Refrigeration Inc. (USA) v. Lars C. Matthiesen, UfR 1996.937 H (Supreme Court of Denmark 30 April 1996) 376
Sallen v. Corinthians Licenciamentos LTDA, 273 F.3d 14, 60 U.S.P.Q.2d 1941 (1st Cir. 2001)..... 117
Schnapp v. McBride, 64 F.Supp.2d 608, 612 FN9 (E.D.La. 1998)..... 193
School of Visual Arts v. Kuprewicz, 3 Misc.3d 278, 771 N.Y.S.2d 804 (N.Y.Sup. Dec 22, 2003)..... 289
Scientology v. Dataweb B.V. & Karin Spaink (Court of Appeal of Hague, Chamber M C-5, No. 99/1040, 4 September 2003)..... 377
Sct. Albans City and District Council v. International Computers Ltd, [1997] F.S.R. 251, [1996] 4 All ER 481 (English Court of Appeal July 1996) 390
Shen-Har Investment & Development Ltd. (Israel) v. Fa. Edelstein Pfanzen (Germany), UfR 1988.426 Ø (Easter Appeal Court 14 December 1987)..... 413
Shevill v.Presse Alliance SA, [1995] 2 A.C. 18, 1995 E.C.R. I-415, [1995] E.M.L.R. 543, (E.C.J. Case C-68/93, 1995) 240, 398
Shirley Jean Nielsen (Nevada, USA) v. Margot Engsig-Karup (Denmark), UfR 1977.887 V (Western Appeal Court 22 July 1977)..... 415, 418
Sidney Blumenthal v. Matt Drudge, 992 F.Supp. 44 (D.D.C. 1998) 227, 252
Simon v. Arizona Board of Regents, 28 Med.L.Rptr. 1240 (Ariz.Sup. 1999)..... 236, 254
Skandinavisk Salgs Service ApS v. S (Sverige), UfR 2000.493 Ø (Easter Appeal Court 30 November 1999) 409
Soda v. Alvarez-Machain et. al., 542 U.S. 692, 732 (US June 2004) 101, 123, 124, 125

Soma Medical International v. Standard Chartered Bank, 196 F.3d 1292 (10th Cir. (Utah) Dec 1999) 120, 131, 178
Sotelo v. DirectRevenue, LLC, 384 F.Supp.2d 1219 (N.D.Ill. Aug 29, 2005) 289
Spaan verpackung G.m.b.H. (Germany) v. Superfos Gødning A/S, UfR 1990.295 H (Supreme Court of Denmark 12 February 1990) 389
Specht v Netscape Communications Corp, 150 F.Supp.2d 585 (S.D.N.Y., July 2001) ... 392
Specht v Netscape Communications Corp, 306 F.3d 17 (U.S. Appeals Court for 6th Circuit October 2002) 392
Spedition Network ApS v. Klaipedoes Litranspedas (Lithuania), UfR 2001.2103 SH (The Maritime and Commercial Court in Copenhagen 20 June 2001) 377
Sports Authority Michigan, Inc. v. Justballs, Inc., 97 F.Supp.2d 806 (E.D.Mich. 2000) . 188
Standard Knitting, Ltd. v. Outside Design, Inc., 2000 WL 804434 (E.D.Pa. 2000) 188
State of Minnesota v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn.App. 1997) ... 184
Steen Sahl Christensen v. K/S CEVO-Invest X, UfR 1997.985 Ø (Eastern Appeal Court 11 April 1997) 376
Sterling Drug, Inc. v. Bayer AG, 14 F.3d 733 (2nd Cir. 1994) 118
Stomp, Inc. v. NeatO, LLC., 61 F.Supp.2d 1074 (C.D.Cal. 1999) 184, 188
Swafford v. Memphis Individual Practice Ass, 1998 WL 281935, 1998 Tenn.App. LEXIS 361 (Tenn.Ct. App.1998) 233, 253
Swarovski Optik North America v. Euro Optics, 2003 WL 22014581 (D. Rhode Island, August 2003) 119
Tech Heads, Inc. V. Desktop Service Center, Inc., 105 F.Supp.2d 1142 (D.Or. 2000) 184
Telco Communications v. An Apple A Day, 977 F.Supp. 404 (E.D.Va. 1997) 194
Telecompany TDC v. IFPI Danmark (Supreme Court of Denmark, 10 February 2006 – Docket 49/2005) 359
The Apollon, 22 U.S. 362 (U.S. 1824) 16, 101
The Queen v. Jameson, [1896] 2 Q.B. 425, 430 (U.K. Queens Bench, 1896) 113
Thompson v. Handa-Lopec, Inc. 998 F.Supp. 738 (W.D.Tex. 1998) 184
Toby Constructions Products Pty Ltd v Computa Bar (Sales) Pty Ltd, 77 FLR 377, [1983] 2 NSWLR 48 (Supreme Court of New South Wales, 1983) 390
Topdanmark Forsikring A/S v. Rentokil Svenska AB, UfR 1996.1547 Ø (Easter Appeal Court 30 September 1996) 394
Trelleborg Aktiebolag (Sweden) v. Danske Gasværkers Tjære Kompani A/S, UfR 1979.1033 SH (The Maritime and Commercial Court in Copenhagen 10 July 1979). 393
Tribunale di Ascoli Piceno v. Gambelli, (E.C.J. C-243/01 of 6 November 2003) 213
Triplex S.p.A. (Italy) v. Haka-Kirk Husholdningsmaskiner A/S under konkurs, UfR 1972.714 H (Supreme Court of Denmark 6 June 1972) 413
Tweede Algemeene Verzekering Maatschappij (Netherlands) v. Forsikringsaktieselskabet "Danske Atlas", UfR 1921.622 H (Supreme Court of Denmark 2 May 1921) 376
Twentieth Century Fox v. iCraveTV, 2000 US Dist Lexis 11670, 53 U.S.P.Q.2d (BNA)

1831 (W.D.Pa, Feb. 8, 2000) 212, 222, 247, 326, 330
U.S. v Scott Levine (United States District Court, E.D. Arkansas. (Little Rock) Feb 2006) 353
UfR 1921.855 Ø (Easter Appeal Court 18 May 1921 - Kære IV nr. 203/1921) 397
United States of America v. Yousef, 327 F.3d 56 (2nd Cir 2003) 122
Universal Boards GmbH & Co. KG. v. Heise Zeitschriften Verlag GmhH & Co. KG (Landgericht Hamburg, 20. September 2005 (Zivilkammer 24) – Docket No. 324 O 721/05) 205
Viasat A/S and Canal Digital Danmark A/S v. A (Danish citizen with residence in Columbia), UfR 2002.405 H (Supreme Court of Denmark, 27 November 2002) 290, 397
Ward Group v. Brodie & Stone, 143 FCR 479, [2005] FCA 471 (Federal Court of Australia, Victoria Dist., April 2005) 106
Weber v. Jolly Hotels, 977 F.Supp 327, 333 (D.N.J. 1997) 190
West India Fruit and Steamship Comp. v. Seafarers International Union of North America, Atlantic & Gulf District, 130 NLRB 343, 350-364 (National Labor Relations Board, 1961) 113
Westcode, Inc. v. RBE Electronic, Inc, 2000 WL 124566 (E.D.Pa. 2000) 138
William Benz v. Compania Naviera Hidalgo, S.A., 353 US 138, 144 (US 1957) 113
Winfield Collection, Ltd. v. McCauley, 105 F.Supp.2d 746 (E.D.Mich. 2000) 181, 195
Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F.Supp.2d 1181 (N.D.Cal., November 7, 2001) 226, 266, 268
Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 145 F.Supp.2d 1168 (N.D.Cal. Jun 07, 2001) 266
Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 379 F.3d 1120 (9th Cir. 23 august 2004 – No. 01-17424) 259, 266, 267
Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 399 F.3d 1010 (9th Cir 2005) 260, 267
Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199 (9th Cir. Jan. 12, 2006) 267, 268, 269, 270, 271, 272, 273
Young v. New Haven Advocate, 315 F.3d 256 (4th Cir. Dec. 13, 2002) 246
Young v. New Haven Advocate, 538 U.S. 1035, 123 S.Ct. 2092 (US Supreme Court, May 19, 2003 – Doc. 02-1394) 246
Yousef Abdul Latif Jameel v Dow Jones & Co Inc., [2005] 2 WLR 1614, [2005] Q.B. 946, [2005] E.M.L.R. 16, [2005] EWCA Civ 75 (Court of Appeal, 3 February 2005) 241, 242
Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. (Va) 1997) 182, 227
Zeran v. America Online, Inc., 524 U.S. 937 (U.S. 1998) 182
Zippo Manufacturing Comp. v. Zippo Dot Com, Inc., 952 F.Supp. 1119 (W.D. Pa. 1997) 120, 130, 131, 135, 137, 139, 160, 175, 177, 178, 179, 180, 181, 187, 189, 190, 191, 192, 195, 196, 201, 372, 385
Zürich Forsikring, Randers afdeling v. Hanne Enger, UfR 1992.645 V (Western Appeal

Court 14. April 1992).....383, 387

ooo000ooo

Danish Cases by normal Danish Citations-method (only <case-report, year and page>):

UfR 1913.721 - Andelsanstalten "Vort Land"
UfR 1920.626 Ø - Købmand Bernhard Petersen v. Købmand P.J. Torfason
UfR 1921.622 H - Tweede Algemeene Verzekering Maatschappij v. Forsikringsaktieselskabet "Danske Atlas"
UfR 1921.908 SH - Handelsfirmaet Vacuum Oil Co A/S v. R Mithassel
UfR 1925.453 SH - A/S Frederik Fiedler v. Firmaet E. Zoubir
UfR 1926.17 H - Flensburger Volksbank A.G. v. Firmaet Jacob Sørensen & Co
UfR 1926.84 H - Firmaet Harald Kjær & Co v. Rederiet Nielsen & Thorden O/Y, Forsikrings-Aktieselskabet Urania v. "Madrid, Sociedad anonima de reaguros"
UfR 1927.516 SH - Islandsk Kompagni A/S v. Oskar Halldorsson
UfR 1930.402 Ø - Firmaet M Friis-Møller & Co v. Firmaet Tandberg & Wigeland
UfR 1932.645 Ø - I.H. Nordgren v. Rederiaktiebolaget "Högmarsåo"
UfR 1938.1094 Ø - Poul Erik Andersen v. William Mønster
UfR 1940.156 Ø - Prosecutor v. Erik Georg Gotthards
UfR 1940.454 H - Alfred Leopold v. Carl Davidsen
UfR 1942.660 SH - Nordisk Fjer A/S v. Firma Samuel Motzen
UfR 1945.393 Ø - Aage Thorning-Christensen v. Ella Hartvig Henriksen
UfR 1947.187 Ø - Erik Fiehn v. A/B Wivefilm
UfR 1951.1117 SH - Københavns ny Tømmer-Handel A/S v. Rederiet for m/s "Alma"
UfR 1954.609 SH - A/S Jølving v. firmaet Wallengreen & Co (Sweden)
UfR 1955.1079 SH - A/S Svendborg Kasein v. Etablissements Freddy Baines
UfR 1956.657 H - A/S Svendborg Kasein v. Freddy Baines S.A.
UfR 1957.613 V - Gunnar Quistgaard Vemb v. L. Egebjerg
UfR 1960.434 SH - Nordisk Rederiaktieselskab v. Firma Terwogt & Lagers
UfR 1962.247 H - Firma Karl O. Helm v. H.A. Hagbarth A/S
UfR 1964.224 H - Direktoratet for Københavns skattevæsen v. Poul Ingvar Steen
UfR 1964.228 H - Brunswick A.G. v. C.E. Jensen
UfR 1968.336 V - Eti-Tuber A/S v. Firma Theodor Klass
UfR 1968.384 H - Bjørn Bartig v. Den Danske Landmandsbank A/S
UfR 1971.512 V - Johann H. Anthon A/S v. Bogesundsmaskiner AB
UfR 1972.1031 SH - Forsikringsselskabet Nye Danske Lloyd v. Stausberg ingenieurbau G.m.b.H., Scan-Report A/S v. Forum Annonsbyrå AB

UfR 1972.714 H - Triplex S.p.A. v. Haka-Kirk Husholdningsmaskiner A/S under konkurs
UfR 1973.206 V - Bent Bjerregaard Thomsens konkursbo v. Astramaris Schifahrtskontor G.m.b.H.
UfR 1974.548 H - Inter System Transport Ltd. v. Hans Erik Harbos konkursbo
UfR 1975.428 H - ASX 265 A/S v. Ulrik Flening
UfR 1977.395 Ø - Niels Mousten Vestergaard v. European Homes B.V. & European Construction B.V.
UfR 1977.887 V - Shirley Jean Nielsen v. Margot Engsig-Karup
UfR 1978.1003 Ø - Prosecutor v. T
UfR 1978.575 V - Bejle Gardiner I/S under konkurs v. Eilermark A.G.
UfR 1978.863 Ø - Ole Bruun ApS v. Schmict O.H.G. Lederfabrik und Kunststoffwerke
UfR 1978.876 H - Firma Electronic v. Konkursboet Stenløse Plastic
UfR 1979.1033 SH - Trelleborg Aktiebolag v. Danske Gasværkers Tjære Kompani A/S
UfR 1979.616 SH - A/S N. Foss Electric v. John Shields (England)
UfR 1982.220 V - Orla Stenhøj v. Eksportkreditrådet
UfR 1982.266 Ø - Bent Manholm v. Andalucia International Real Estate
UfR 1982.441 H - Jørgen Jakob Hempel v. I.C.H. Industrial and Commercial Holding A/S
UfR 1984.324 V - Kreativt Center A/S v. Karen Margrethe Reiff
UfR 1985.709 Ø - Dansk-spansk vinimport D.S.V. A/S under konkurs v. Anselm Mayrs dødsbo
UfR 1985.904 H - Coprosider S.p.A. (Italy) v. Vølund Energiteknik A/S
UfR 1986.922 H - Dow Corning International Ltd. v. Dansk Tyggegummifabrik A/S
UfR 1987.14 H - Bauherrengemeinschaft v. Konkursboet Bent Iversen,
UfR 1987.216 Ø - Prosecutor v. T
UfR 1987.690 H - Industriaktiebolaget EUROC v. Inger Topsøe & Swegon AB
UfR 1988.426 Ø - Shen-Har Investment & Development Ltd. v. Fa. Edelstein Pfanzen
UfR 1988.579 SH - Capstan Shipping Ltd. ApS v. ScanPly International Wood Products Ltd.
UfR 1989.969 Ø - Irvin B. Gold v. Chevron Petroleum Company of Denmark
UfR 1990.295 H - Spaan verpackung G.m.b.H. v. Superfos Gødning A/S
UfR 1990.408 V - Klapmølle Dambrug v. B.S. Forellen
UfR 1990.475 V - Allan Haugsted v. Firma Maretec A.G.
UfR 1990.597 H - Felixstowe Dock & Railway Co. v. Investorgruppen Danmark K/S and A/S Det Østasiatiske Kompagni
UfR 1990.70 H - Prosecutor v. T
UfR 1991.779 Ø - Erik Mølgaard Petersen v. Helge Otto Jørgensen
UfR 1992.645 V - Zürich Forsikring, Randers afdeling v. Hanne Enger
UfR 1992.746 H - Jørgen Schmidt Trading A/S v. Smedbo AB
UfR 1996.1538 Ø - Prosecutor v. T (Courts of Appeals for Eastern District, 1996)
UfR 1996.1547 Ø - Topdanmark Forsikring A/S v. Rentokil Svenska AB

UfR 1996.356 Ø - Prosecutor v. T
UfR 1996.937 H - Sabroe Refrigeration A/S and Sabro Refrigeration Inc. v. Lars C. Matthiesen
UfR 1996.950 SH - Kilchem Adriatic of 25/6/1993 A/S v. Office National de l'Huile
UfR 1996.979 Ø - Prosecutor v. T (Courts of Appeals for Eastern District, 1996)
UfR 1997.565 SH - H.H.Andersen Konfektion Aps v. Textilwerke Ganahl A.G.
UfR 1997.707 H - Poul Erik Bøjden v. Bikuben Girobank A/S
UfR 1997.985 Ø - Steen Sahl Christensen v. K/S CEVO-Invest X
UfR 1998.728 SH - Con-Mec A/S v. Fournais Handels- & Ingeniørfirma A/S
UfR 1999.177 V - Prosecutor v. T
UfR 1999.88 H - S. Bjerregaard & Sønner Fiskeeksport A/S under konkurs v. Gulf Fish Trading Ltd.
UfR 1999.939 H - Pakistans Ambassade v. Shah Travel
UfR 2000.1181 Ø - Prosecutor v. T
UfR 2000.1450 Ø - Prosecutor v. T
UfR 2000.1635 Ø - Alfa-Bank v. S
UfR 2000.493 Ø - Skandinavisk Salgs Service ApS v. S (Sverige), (Easter Appeal Court 30 November 1999)
UfR 2001.1039 H - Damstahl A/S v. A.T.I. s.r.l.
UfR 2001.1529 H - CEAG Sicherheitstechnik GmbH v. Eksportkreditfonden EKF
UfR 2001.2103 SH - Spedition Network ApS v. Klaipedoes Litranspedas
UfR 2001.2186 Ø - Canal Digital Danmark A/S v. Hans Magnus Carlsson
UfR 2001.2573 Ø - Prosecutor v. T
UfR 2001.432 SH - Morgan Crucible Company Plc. v. A.B. Svejseteknik ApS
UfR 2001.697 Ø - A v. Baan Nordic A/S (tidligere Beologic A/S)
UfR 2002.1370 Ø - 1st Mover Aps v. Direct Hedge S.A.
UfR 2002.1676 Ø - Lund-Hansen Advokatvirksomhed ApS v. Benedikte Moeskær
UfR 2002.290 H - Landsbanki Islands Lögfrændingadeild v. Akzo Nobel Chemicals B.V.
UfR 2002.405 H - Viasat A/S and Canal Digital Danmark A/S v. A
UfR 2002.424 SH - PIL-Pak A/S v. Crownson Fabrics Ltd.
UfR 2003.1063 SH - Danske Dagblades Forening v. Newsbooster
UfR 2003.136 V - K v. Fogedretten i X-by
UfR 2005.3446 H - Rigsadvokaten v. Teleselskabet [tele-company] Debitel

VLT 1957.292 - Aktieselskabet Havnemøllen v. Firma Je-Ba v/J. Jensen

13. Index

A

ABA jurisdiction Rules, 128
Access Control List, 80
Active personality principle, 16, 102, 104
Actor sequitur forum rei, 115, 392
Additional Protocol, cybercrimes, 313
Address Resolution Protocol, 78
Address Resolution Protocol attacks, 81
Age limit in international criminal law, 300
Als Scan Test, 177
Anonymizers, 220
Anycast, 73
Application and vulnerability scans, 77
Application Layer, 38, 45
ARP, 81
ARPA, 46
ARPANET, 46
ARPA-system, 44
Association Amicale des Déportés d'Auschwitz et de S Camps de Haute Silesie, 261
Aut dedere aut judicare, 321, 330, 331
Authentication mechanism, 62

B

Backbone Network Service, 47
Basic assumptions any host must follow, 63
Basic Requirements in the Internet Architecture Suit, 62
Bent-pipe satellites, 304
Berners-Lee, 2, 12, 35, 47, 75, 110, 377
Best effort, 74
Bogotá Declaration, 302
Breach jurisdiction rule, Denmark jurisdiction, 393
Breach of law involving claim of penalty, damages or redress of a wrong, Denmark jurisdiction, 393
Bridge, 58
Broadcast amplification attacks, 81
Brunswick, Duke of - principle, 227
Brunt of the harm, California courts, 269
Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, 367
Budapest Convention, see Cybercrime Convention, 281

C

Cerf, 11, 46, 86, 88, 93, 98, 110, 112, 264, 378
Chapter 22 of the Danish Civil Procedure Code, 438
Chicago Convention, 319
Child pornography, Denmark, 362
CIDR, 75
Civil jurisdiction, 114
CIX, 47
Clarke Orbit, 22, 42, 109, 302, 303, 304, 305
Classless Inter-Domain Routing, 75
Close link, vi, 145, 172, 328, 369
Closeness, 5, 6, 92, 112, 115, 146, 156, 157, 160, 161, 162, 164, 166, 169, 251, 325, 326

Code is law, 6
Commerce Clause, U.S., 213
Commercial Information Interchange, 47
Communications Decency Act of 1996, U.S., Immunizing Internet Service Providers, 226
Communications satellites, 302
Communications Subnet, 38
Communications subnetwork, 45
Computer Science Network, 46
Concurrent jurisdiction, 146, 170, 171, 296, 297, 323
Congestion Control, 66
Consumer agreement in Danish law, 400
Consumer contract, Denmark jurisdiction, 399
Contents of Messages, 3
Contracts, Denmark jurisdiction, 388
Contravention, France, 272
Convention Against Transnational Organized Crime, 120, 294
Convention on International Civil Aviation, 319
Convention on Registration of Objects Launched into Outer Space, 306
Convention on the Law of the Sea of 1982, 147, 319
Cookies, 287
COP, 294
Copycats, 148
Copyright, Denmark, 356
Corporations, associations, private institutions and other - business outside ”home jurisdiction” , Denmark jurisdiction, 386
Cracker, 286
Crimes related to Gaining Profit, Denmark, 350
Crimes related to Peace, Privacy and Honor, Denmark, 353
Crimes under the Cybercrime Convention, 310
Criminal jurisdiction, 114
CSNET, 46
CTOC, 294
Customer portion of the System, 45
Customer self-identification, 221
Cybercrime Conv, additional crimes in Protocol, 313
Cybercrime Conv, art 11, 311
Cybercrime Conv, art 18, 319
Cybercrime Conv, art 19, 320
Cybercrime Conv, art 21, 312
Cybercrime Conv, art 22, 316, 326
Cybercrime Conv, art 22(1)(a)-(c), 317
Cybercrime Conv, art 22(1)(d), 320
Cybercrime Conv, art 22(2), 321
Cybercrime Conv, art 22(3), 322
Cybercrime Conv, art 22(4), 322
Cybercrime Conv, art 22(5), 323
Cybercrime Conv, art 24, 322, 330
Cybercrime Conv, art 30, 320
Cybercrime Conv, art 32, 324
Cybercrime Conv, art 38, 324
Cybercrime Conv, art 39, 324
Cybercrime Conv, Extradition, 322
CyberCrime Conv, Jurisdiction, 324
Cybercrime Conv, serious offence, 312
Cybercrime conv, Traffic data, 37
Cybercrime Convention and its Protocol, Denmark’s Reservations to the, 459
Cybercrime Convention of 23 November 2001, 281
Cybercrime Convention, possession or control, 319
Cybercrime Convention, relating to such service, 319

Cybercrime Convention, some common minimum safeguards, 313
Cybercrime, Jurisdiction under public international law, 290
Cybercrime, offence occur on its territory, 326
Cybercrimes, 282, 310, 313
Cyberpiracy, 311
Cyberracism, 312
Cybersmuts, 312
Cyberspace Jurisdiction in the U.S., 196
Cybersquatting, 311
Cybertorts, 312

D

Danish Civil Procedure Code § 248, 379
Danish Civil Procedure Code, chapter 22, 438
DARPA, 46
Data, 14
Data interference, Cybercrime Conv., 150
Data Link Layer, 45
Datagram, 38
Datakriminalitet, 344
Decapsulation, 62
Dedere aut judicare, 330, 331
DHCP, 81
Digital, 14
Distance contracts, 372, 400, 401, 402
Distance sales, 401
Distanceaftaler [distance contract], 401
Division of jurisdictional rules, 117
Domain name, 51
Domain Name System, 34
Dormant Commerce Clause, U.S., 213
Double jeopardy, 161, 297, 331, 332
Dual stack, 85
DVDjon, 360
DVD-Zones, 287
Dynamic Host Configuration Protocol attacks, 81
Dynamic packet filters, 59

E

E.F. Tidende, 462
E.U. Tidende, 462
EF-domskonventionen, 462
Effect Doctrine, 17, 18, 102, 106, 396
Effect test, 164, 194, 250, 326, 372, 397
Encapsulation, 61
End Systems, 58
Enforcement/Execution, Denmark, 418
Enslavement, ICC-statute, 149
ESs, 58
Execution, Denmark, 418
Extension headers, IPv6, 71
Extradite, 276, 296, 297, 317, 321, 322, 330, 331, 335, 348
Extradite or prosecute, 330
Extradition, 296
Extreme foreign punishment, 334

F

F.T., 462
First Amendment of the U.S. Constitution, 226
Five general business models for websites, 190
Fixed Satellite Service, 304
Fjernsalg [distance sales], 401
Flags, 67
Flooding, 83
Flow Label, 70
Folketings Tidende, 462
Foreign punishment, 334
Foreigner, procedural, Denmark, 143
Forgery, Cybercrime Conv., 150

Forgery, Denmark, 360
Forum non-convenience doctrine, not in Denmark, 368
Fragment Offset, 67
Fragmentation attacks, 80
Frame, 58
Fraud, Cybercrime Conv., 151
Fraud, data, Denmark, 351
Free orbit of spacecraft, 301
Free speech, 15, 19, 41, 42, 104, 107, 155, 204, 205, 209, 213, 216, 223, 226, 262, 270, 279, 313, 314, 325, 421
Free Speech Online, 222
Freedom of expression, 14, 103, 158, 159, 170, 275, 308, 309, 316, 341
French Penal Code R645-1, 272
FSS, 304

G

Gateway, 53
Gator-2003-case, 134
General jurisdiction, 118, 134, 139, 325
General Jurisdiction, sufficient closeness, 160
Geneva Declaration of Principles, 23, 31, 36, 278, 341
GeoIP, 221
Geo-location, 218
Geostationary Earth Orbit, 303
Geosynchronous Orbit Satellites, 22
Geo-tracking, 218
GII, 13
Global Jurisdiction, v, vi, 5, 95, 116, 118, 128, 129, 143, 146, 156, 165, 167, 168, 169, 170, 171, 172, 275, 277, 290, 312, 325, 329, 402
Global Jurisdiction - Definition, v
Global Jurisdiction, ABA Report on, 128
Global Jurisdiction, sufficient closeness, 156
Global Survey of Cybercrime Laws, 307
Godsværnetinget, 409
Goods-jurisdiction-rule [“Godsværnetinget’] , Denmark jurisdiction, 409
Grave breaches, 127, 152
GSO, 303
GSOs, 22

H

Hacking, 285
Hacking, Denmark, 350
Hacktivism, 286
Header Checksum, 67
Header manipulation, 80
Henrik’s 1st Base: Pure Online (cross-border), 1
Henrik’s 2nd Base: No one owns Cyberspace, 1
Henrik’s 3rd Base: The discussion of Cyberspace issues should be limited, 2
Henrik’s 4th Base: No Worldwide Jurisdiction besides Universal Jurisdiction, 5
Henrik’s 5th Base: Internet protocols have become customary law, 6
Henrik’s 6th Base: Computer programmers & lawyers are rule-makers for Cyberspace, 7
Hierarchy for states having concurrent jurisdiction, terrorism, 323
High Sea, 10, 34, 40, 112, 150, 274, 275, 278, 341
Host Process, 38, 45
Host-to-Host (Service) Layer, 38
HTTP, 98

Human rights, Cyberspace, vi, 24, 31, 33, 100, 145, 261, 275, 285, 286, 308, 313, 325, 331, 335, 338
Hypertext transfer protocol, 98

I

IAB, 27
IANA, 27, 44
ICANN, 27, 30
ICC Statute's Jurisdictional Rules, 298
ICCPR, 158, 159
IESG, 43
IETF, 26, 43
IHL, 65
In rem jurisdiction, 116
Indecency, Denmark, 361
Information on Web-pages, 4
Information Warfare, 76, 152, 284, 301, 337
InfoSplit, 219
Insult or breach jurisdiction rule, Denmark jurisdiction, 393
INTELSAT, 28
Intelsat Ltd, 28, 30
Interception, Cybercrime Conv., 150
International Covenant on Civil and Political Rights, 14, 15, 36, 41, 103, 104, 158, 223, 308, 313, 331
International Criminal Court, 298
International Criminal Court, no U.S. cooperation, 301
International Organization for Standardization, 45
International Standards Organization, 26, 45
International Telecommunications Satellite Organization, 27
International Telecommunications Union, 9, 24, 39, 110
Internet - Definition, 9
Internet Architecture Board, 27, 43
Internet Architecture Suit, 62
Internet Assigned Numbers Authority, 27, 44
Internet Corporation for Assigned Names and Numbers, 27
Internet Engineering Steering Group, 43
Internet Engineering Task Force, 26, 43
Internet governance - definition, 22
Internet Header Length, 65
Internet in the sky, 304
Internet Layer, 62
Internet Layer spoofing, 80
Internet Protocol, IP, 6
Internet protocols have become customary law, 6
Internet Research Task Force, 44
Internet Society, 27, 43
Intranet, 49
Intranets, 58
Intrusion Detection System, 81
IP, 6
IP 4to6, 83
IP 6to4, 83
IP address, 51
IP datagram, 38
IP fragmentation technique, 68
IP Security - Attacks, 76
IP Spoofing, 75
IP-level security, 62
IPng, 37
IPv4 fragmentation, 80
IPv4 of 1983, 64
IPv6 of 1996, 37, 69
IPv6, extension headers, 71
IRTF, 44
ISO, 26, 30, 45
ISOC, 27
IT-kriminalitet, 344
ITSO, 27, 30

ITU, 24, 30
ITU-D, 25
ITU-R, 25
ITU-T, 25
IW, 284

J

Joined declaration issued by the European Parliament and Commission at the time the Regulation was passed - Statement on Articles 15 and 73, 372
Journal of Law, 462
Jurisdiction in public international law - categories, 102
Jurisdiction, CyberCrime Conv,, 324
Jurisdictional rules, division of, 117
Juristen, 462
Justice Souter in *Denver*, 196

K

Karnov Lovsamling, 462
Keylogging, 283
Keystroke logging, 283
Koogle, 261

L

L'Union des Etudiants Juifs de France, 259
L2TP, 61
La Ligue contre le Racisme et L'Antisemitisme, 259
Lakin-case, 138
Launching satellite state, 307
Law of Conflicts - Definition, 11
Law of the Sea, 147, 278, 317, 319
Legality, principle of, 292
LICRA, Yahoo-case, 259
Link, v, 5, 26, 29, 58, 60, 64, 66, 71, 73, 79, 96, 113, 143, 146, 195, 234, 319, 326, 372, 376, 378, 382, 384, 408, 422
Locus delicti, 318
Loi Toubon, 263
Loopback, 73
Lowest limit for Outer Space, 301

M

MAE's, 49
Man-in-the-middle attacks, 82
Master International Frequency Register, 25
Maximum transfer unit, 62
MaxMind, 221
Means of Payment, Denmark, 360
Metropolitan area exchanges, 49
Microwave towers in the sky, 304
Middle layer, 45
Minimum test, 325
Minors in the sky, 304
MIPv6, 91
Misuse of devices, Cybercrime Conv., 151
Mobile IP Version 6, 91
Mobile Satellite Service, 304
Montego Bay Convention, 147, 150, 319
Mootness Doctrine, U.S., 269
Mosaic, 47
Most serious crimes, 300
Mouvement contre le racisme et Pour L'amitié entre les Peuples, 261
MSS, 304
MTU, 62
Multicast, 73
Multiple publication rule from Brunswick, 228
Municipal law - Definition, 11
Music of the Law, vii

N

NAPs, 47
NAT, 78
National Conference of Commissioners on Uniform State Laws, 231
National jurisdiction, 116, 118, 153
National jurisdiction, sufficient closeness, 153
National Science Foundation, 46
Nationality principle, 16, 102
Natural persons who run a business, Denmark jurisdiction, 380
NBMA, 85
NCCUSL, 231
Ne bis in idem, 297, 331, 333
Network Access Points, 47
Network Address Translation, 78
Network layers, 38
Network Layers, 45
Network Terms, 58
Next Header - IPv6, 70
NGSO, 302
Node, 38, 50
Nonbroadcast multiaccess, 85
Non-Geostationary Earth Orbit, 302
NSF, 46
Nulla poena sine lege, 292
Nullum crimen sine lege, 292

O

O.J., 462
OASC, 47
Objective Territoriality Principle, 17, 102
Occurring “in” or “on” the territory, 318
Office of Advanced Scientific Computing, 47
Online auction sites, Denmark, 403
Online Newspapers, 203
Open system, 49
Open Systems Interconnection, 44
Ophavsret, Denmark, 356
Ophavsretloven, 462
OSI, 44
OSI model, 26
OSI Reference Model, 45
Outer Space, 34, 301, 302, 306, 307, 337
Outer Space Treaty, 302
Oxford Experiments, 182

P

Packet Filtering Bridge, 59
Palermo Treaty, 120, 127, 160, 294, 295
Parallel treaty between Denmark and the E.U., 367, 442
Passive nationality principle, 17, 102, 325
Passive personality principle, 17, 102, 325
Patriot Act, 399
Payload Length, 70
Peering, 49
Persistent Identification Element, 287
PGP, 47
Pharming, 283
Phishing, 283
Physical Layer, 45
Physical, Data Link, 38
PIE, 287
Ping sweeps, 76
Pipe-lines, 106
Piracy, Denmark, 356
Plenipot (ITU), 25
Point-to-Point packets, 61
Port, 51
Port scans, 77
Possession or control, Cybercrime Convention, 319

PPP packets, 61
Precedence Subfield, 65
Predictability, 6
Presentation Layer, 38, 45
Pretty Good Privacy, 47
Principle of legality, 292
Privacy facility, 62
Private International Law - Definition, 11
Property [, 409, 415
Protective theory, 106
Protective Theory, 17, 18, 103
Protocol, key features of, 49
Protocols, 49
Protocols of the Internet - categories, 44
Public international law - Definition, 10
Pure Online, v, vi, 1, 16, 101, 104, 116, 129, 143, 145, 153, 156, 157, 163, 166, 167, 172, 173, 203, 206, 208, 210, 326, 365, 366, 368, 382, 383
Pure Online - Definition, v

Q

QoS, 74
Quality of Service, 74
Quasi-in-rem jurisdiction, 116
Queue Service, 66

R

Racist and xenophobic material, 309
Radiocommunication Sector, 25
Reasonableness, vi, 5, 6, 92, 112, 113, 130, 139, 157, 164, 169, 170, 172, 252, 257, 289, 299, 323, 326, 330, 340, 396
Reconnaissance, 76
Rehearing en banc, California, 260
Remote sensing, 158
Reports related to the Brussels Convention, the Lugano Convention and the E.U. Regulation 44/2001, 367
Request for Comment - Definition, 43
Restricted jurisdiction, 121
Restricted Jurisdiction, 156
Restricted Jurisdiction, sufficient closeness, 156
Retraction Rule, 231, 256, 257, 428
Retraction Statute, Alabama, 435
Retraction Statute, California, 436
Retsplejeloven, 462
Retsplejeloven § 248, 379
RFC, 43
Ripeness, U.S., 269
RMS, 158
Robustness Principle, 62, 314
Router, 50, 58
Router, ordinary, 59
Router, screening, 59
Routing attacks, 81
Rpl., 462
Rules on Cross-Border, 209

S

San Sebastian Convention, 367
SARA, 182
Satellite, 14, 21, 22, 29, 34, 37, 42, 46, 96, 109, 110, 276, 277, 303, 304, 305, 317, 318, 321, 327, 328, 337
Satellite communication, 303
Satellites for data transport in Outer Space, 301
SATNET, 46
ScatterChat, 286
Schengen Treaty, 332
Segment, 53
Separate Satellite Systems, 29
Serious crimes in Palermo Treaty, 295
Serious Crimes under international law,

127
Serious offence, Cybercrime Conv, 312
Session Layer, 38, 45
Sexual Morality, Denmark, 361
SHT, 462
Single Publication, 215, 216, 227, 228, 229, 230, 231, 232, 233, 244, 254, 255, 256, 257, 424, 425, 427, 483
Single Publication Model Act, 229
Single Publication Model Act, U.S. States with statutes on basis of the, 424
Single Publication Rule, 215, 256
Single Publication Rule, California, 427
Single Publication Rule, U.S. States by case law that have adopted the, 425
Smurf, 81
Sniffing, 82
Sovereignty, Henkin, 157
Spacecraft, 302
Spam, 287
Specific jurisdiction, 119, 325
Specific Jurisdiction, sufficient closeness, 160
Spyware, 282
SRI, 46
Stanford Research Institute, 46
Stanford-Proposal, 281, 310, 317
Stare Decisis Doctrine, not in Denmark, 343
State sovereignty, 9
Stateful Packet Filters, 59
Sted [~ "place"], , Denmark jurisdiction, 382
Straffeloven, 462
Subjective Territoriality Principle, 16, 102, 104
Subnet, 45, 90
Subnet Masks, 51
Sufficient closeness, vi, 130, 146, 153, 156, 157, 160, 162, 164, 166, 172, 299, 421
Switchboard-in-the-sky, 304
System interference, Cybercrime Conv., 150

T

Table 1.1 - Public International Law Principles involved, 17
Table 2.1 - Internet Evolutions, 48
Table 2.2 - Operational Networks on the Internet, 48
Table 2.3 - TCP Header (20 octets and 32 bit), 53
Table 2.4 - IPv4 Header (20 octets and 32 bits), 53
Table 2.5 - IPv6 Header (40 octets and 31 bit), 53
Table 2.6 – ARPA – OSI Layers, 56
Table 2.7 - IPv6 Fragment Header, 72
Table 2.8 - Comparison of IPv4 & IPv6 Headers, 84
Table 3.1 - Jurisdiction to prescribe, 105
Table 4.1 – Zippo's Interactive Scale, 180
Table 4.2 – Cases which exercises jurisdiction and where web-content has been referred thoroughly in decision, 184
Table 4.3, 185
Table 5.1 - Where new law may be needed, 208
Table 5.2 - Public International Law Principles Involved, 211
Table of Frequency Allocations, 25
Taxman, 182
TBDF, 158
TCP, 6
TCP/IP, 6

Telecommunication, 45
Telecommunication Development Sector, 25
Telecommunication Standardization Sector, 25
Telecommunications - Definition, 13
Territorial sovereignty, 321
Territoriality Principle, 16, 102
Theft done by electronic bits-transmission, Denmark, 351
Three Strike rule, 334
Timothy Koogle, 261
Tor, 286
TOS Subfield, 65
Toubon law, 263
Trade/commercial through Internet, 4
Traffic Class, 70
Transborder data flow, 158
Transition, translation, and tunneling mechanisms, 82
Translation, 85
Transmission Control Protocol, 6, 19, 27, 38, 44, 97
Transnational jurisdiction, 116, 120, 160
Transnational Jurisdiction, sufficient closeness, 160
Transport Layer, 38, 45
Transport Layer spoofing, 80
Tunis Agenda, 8, 341, 488
Tunis Commitment, 278
Tunneling, 61
TWOC, 351

U

UDHR, 159
UDP, 38, 54
UfR, 462
Ugeskrift for Retsvæsen, 463
Unauthorized access, 79
Underwater cables used for international Internet traffic, 12
Unicast, 72
Uniform Correction or Clarification of Defamation Act, 231
Uniform Single Publication Model Act, 229
Universal addressing, 74
Universal Declaration of Human Rights, 14, 23, 41, 103, 159, 223, 341
Universal jurisdiction, 5, 117, 121
Universal jurisdiction over criminal acts, 125
Universal Jurisdiction, crime, 293
Universal Jurisdiction, sufficient closeness, 146
Unlawful access to others information or programs, Denmark, 353
Unlawful distributes messages or pictures, Denmark, 356
Unmanned spacecraft, 302
User Datagram Protocol, 38, 54

V

vBNS, 47
Viruses, 82
VLT, 463

W

War crimes, 125, 127, 147, 152, 262, 301
Warehousing, 311
Web-sites (activity level catalog) – U.S. Cases, 181
WGIG, 22
What is a Cybercrime?, 282
What law has to be followed?, 210
Where is the Newspaper published?, 217

World Factbook of Criminal Justice Systems, 307
World Wide Web, 47
Worldwide jurisdiction (see Global Jurisdiction), 118
Worms, 82
WSIS, 22
WSIS Declaration of Principles, 23
www, 47

X

Xenophobic material, 309

Y

Yahoo, 32, 88, 93, 112, 154, 212, 219, 226, 247, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 278, 290, 318, 368, 377, 378, 399, 403, 422
Yahoo! Inc. versus France, 259

Z

Zippo Sliding Scale-Method, 137, 139, 179
Zombie, 283