School of Law
UNIVERSITY OF GEORGIA

Prepare.
Connect.
Lead.

Digital Commons @ University of Georgia School of Law

LLM Theses and Essays

Student Works and Organizations

1-1-1997

LEGAL ASPECTS OF THE INTERNET

ETIENNE PICHAT
University of Georgia School of Law

Repository Citation

PICHAT, ETIENNE, "LEGAL ASPECTS OF THE INTERNET" (1997). *LLM Theses and Essays*. 238.
https://digitalcommons.law.uga.edu/stu_llm/238

This Dissertation is brought to you for free and open access by the Student Works and Organizations at Digital Commons @ University of Georgia School of Law. It has been accepted for inclusion in LLM Theses and Essays by an authorized administrator of Digital Commons @ University of Georgia School of Law. Please share how you have benefited from this access For more information, please contact tstriepe@uga.edu.

K
4L
1997
.P53

Law Library
School of Law
The University of Georgia

The University of Georgia

Alexander Campbell King Law Library

UNIVERSITY OF GEORGIA LAW LIBRARY
3 8425 00347 3878

LEGAL ASPECTS OF THE INTERNET

by

ETIENNE PICHAT
Magistère de Juriste d'Affaires
University of Jean Moulin - Lyon 3
France, 1995

A Thesis Submitted to the Graduate
Faculty of the University of Georgia in the Partial
Fulfillment of the Requirements for the Degree
MASTER OF LAWS

ATHENS, GEORGIA
1997

LAW LIBRARY

LEGAL ASPECTS OF THE

INTERNET

by

ETIENNE PICHAT

Approved:

F. I Fecht Date 6-5-97

Major Professor

Date 5 June 1997

Chairman, Reading Committee

Approved:

Gordhan L. Patel

Graduate Dean

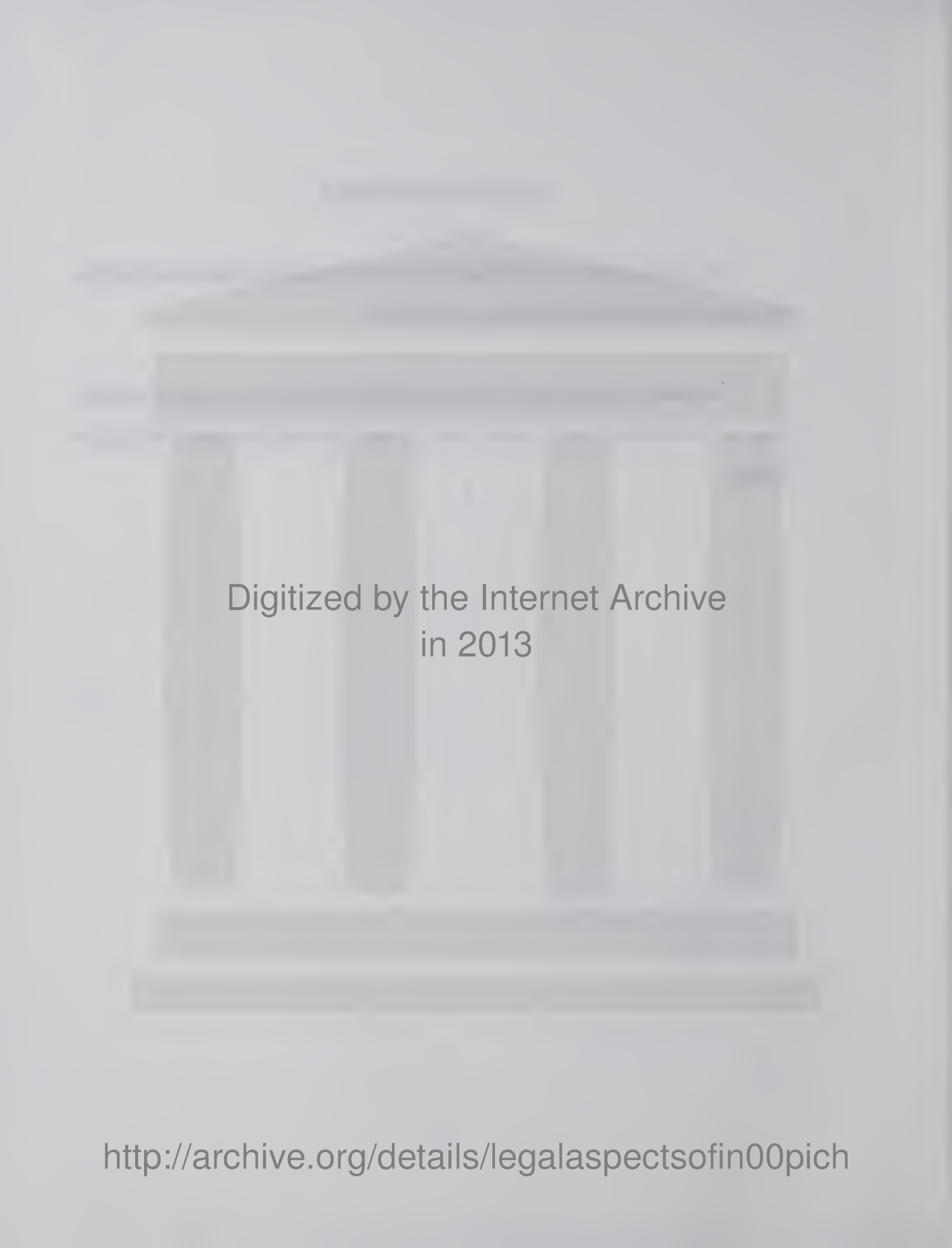
June 6, 1997

Date

ACKNOWLEDGEMENT

The author wishes to acknowledge the helpful and valuable comments and insights of Professor Paul Heald, in the drafting of this thesis.

The author wishes to thank Mademoiselle Virginie Masson for her support and great ideas and Mademoiselle Julie Losman for all the time she spent pertinently checking his English.


Digitized by the Internet Archive
in 2013

http://archive.org/details/legalaspectsofin00pich

TABLE OF CONTENTS

INTRODUCTION

More than 3,000 years ago, Pythagoras, the first philosopher, had already said that all thing are numbers. For him, the Number was both the matter and the model of the world. Today this Number, at the international level has a name: the INTERNET, memory of the world, playing with borders and time zones, abolishing every impediment to the free flow of information. The Internet is based on an international network of computers which allows information pictures, writings, speeches, to be sent all over the world in a few seconds. The world is now a single interconnected society that some have termed a "global village"[1] because the Internet has a remarkable capacity for unifying nations.

In 1957 , the United States Department of Defense (DOD) created the Advanced Research Projects Agency (ARPA), a military research organization to invent a new communication network which would survive military catastrophe. In event of such a disaster, the DOD wanted to be able to maintain links between computers so that military and scientific information could continue to be exchanged with ease. In 1969, Arpanet, the first decentralized computer network, was born, and in the 1970's, research centers and famous universities joined the network: in United States UCLA, MIT, Stanford and Harvard; in Europe the University College in London and the Royal Radar Establishment in Norway.[2]

In 1972, the Internet Working Group was created, directed by Vinton Cerf. It developed the Electronic Mail (E-mail), and in 1979 the first newsgroups appeared,

---

[1] University of Toronto professor Marshall McLuhan coined the term "global village" in the 1960s.

[2] Internet et le web facile, Guide pour Mac & PC, Edition des Mille et Une Nuits (1996).

collectively known as Usenet. Usenet can be described as a huge database of messages, grouped by topic, to which anyone with a computer on the network can have access

In 1986, the National Science Foundation created the NSF-NET because Arpanet had become overloaded. Indeed, from 1984 to 1988, the number of computers connected to the network, now called the Internet, grew from 1,000 to more than 60,000. The Internet arrived in Europe in 1988, and on the 28th of July, l'Institut National de la Recherche Informatique et Automatique *(National Institute for Automatic and Computer Research)*, the first French site was connected. In the following years other countries joined the network: Australia, New Zealand, Argentina . . .

The World Wide Web[3] was proposed in 1989 by Tim Berners-Lee of the Centre Européen de Recherche Nucléaire (CERN, European Center for Nuclear Research). The Web allows one to easily surf [4] the Internet.

In 1991, the NSF authorized the utilization of the Internet for commercial purposes, therefore, the Commercial Internet eXchange (CIX) was created to group together the most important providers[5] of Internet access.

Since 1993, more and more advanced software has been launched to facilitate surfing on the Web. The first program was Mosaïc, soon followed by Netscape and Explorer. Going for a walk on the network had become a child's play. Between 1989 and June 1994, traffic on the web increased up to 2,500%, and sites belonging to commercial companies (those

---

[3] The World Wide Web or Web is a segment of the Internet that organizes information into a series of menu pages linked to other pages.

The author presumes the reader has general familiarity with cyberspace. For the novice, a recommended introduction is Joshua Eddings, How the Internet Works (1994).

[4] To surf means to access electronically information provided by different servers in diverse geographical locations through the use of specialized "browsing" software.

[5] A provider is a point of access and of connection to the internet. A service provider is a company that provides a connection to the Internet.

with address ending with ".com") became greater in number than sites belonging to universities or schools (those with address ending with ".edu")[6].

The Internet is the most visible example of an international computer network. It is distinguished by the fact that no individual or organization owns it and that, over the past few years not just the scientific and academic community but "ordinary" users, private individuals and businesses, have begun to use it widely. The Internet is essentially user-driven, with users, rather than publishers, generating a substantial part of the "content."

A unique characteristic of the Internet is that it functions simultaneously as a medium for publishing and for receiving information. Unlike in the case of traditional media, the Internet supports a variety of communication modes: one-to-one, one-to-many, many-to-many. An Internet user may "speak" or "listen". At any given time, a receiver can and does become a content provider, by responding personally, of his own accord, or by the "re-posting" of content he has previously entered by a third party.

Most individual users do not have permanent direct access to the Internet. They go through an access provider. The term "Internet service provider" is often used generically. Nevertheless, a distinction has to be made between the service of providing access to the Internet (access provider) and the service of hosting content (host service provider). They both connect to the Internet via a leased line, a telecommunication connection made available by the "network operator", such as Bellsouth in the south of the United States, France Telecom in France, or British Telecom in United-Kingdom.

Each computer connected to the Internet must be identified by a network location. Just as one needs to know the physical address of the person they are writing to in order to

---

[6] Internet addresses typically includes a final extension to their "uniform ressource locator" (URL). The most familiar URL extension are ".com", indicating that the accessed computer is commercial; ".edu", educational; "org.", non-profit organization; ".gov", government agency; ".net", networking organization.

An international accord has been signed in Geneva May 1, 1997 to create new domain names. That will bring to an end the lucrative monopoly, until now, held by Network Solutions Inc (NSI) of the US. Then, another seven domain name are available: .firm (business); .store (goods for sale); .web (World Wide Web activities); .arts (culture); .rec (recreation); .info (information); and .nom (individual web sites).

send them mail, a computer must know the Internet address of the machine to which data is to be transmitted. Each computer on the Internet is identified by the Internet Protocol (I.P.), which requires a unique address represented by groups of numbers separated by dots. I.P. addresses are classified by a domain name. Domain names are given and managed by different entities depending on their origin, and the domain are combined into a single group for each country. This group is itself connected to the Internet, and is identified by a two letter code such as <us> for the United-States, <fr> for France and <uk> for United Kingdom. The complete address of a document on the Internet is called a U.R.L., for Universal Resource Locator[7].[8]

Nothing more than a modem and a telephone line are needed to connect a computer to the network, and use by individuals is extensive. A French poll by Mediaangles showed that 480,00 French people are connected to the Internet for at least six hours a week. 31% are connected from their homes, 38% from work. In Germany, there are two millions users. But who exactly are the users? The University of Georgia polled 11,700 American users and, according to the questionnaire, the users earn on average, $ 70,000 a year and are thirty three years old. Sixty eight and a half percent of them are men. This profile of the typical user perhaps explains why fifty-two percent of American firms have plans to be connected to the Internet. All of the companies classified in the "Fortune 500" are already on the World Wide Web.[9]

What are the intentions of these users when they connect their computers to the network? There are two main purposes: navigating the web and using the Electronic-mail, gathering information and communicating.

---

[7] http://www.odci.gov/cia/ for example is the Internet address of the Central Intelligence Agency.

[8] Internet et le web facile, Guide pour Mac & PC, Edition des Mille et Une Nuit (1996).

[9] Le serveur Internet, Document de présentation (1996).

The Web is the area where text, graphics and even sound and video clips may be viewed. Web pages are linked to each other by series of "hyper-links" offering a congenial and highly interactive way of navigating through web content. Just by clicking, you can travel from Paris to New-York, examining from the Musée du Louvre to the Museum of Modern Art. Thanks to very powerful search engines[10] it is possible to find on the web whatever one may be looking for: travel, books, news . For example, lawyers can find a lot of legal information: court decisions[11], articles, access to libraries[12] . . . Another feature of the Web, hypertext[13] enables users, when they "visit" one location (called a page or a site), to have the opportunity to visit any of a number of other related locations, in any of a number of other countries. Frequently, users are unaware that they have even crossed a political border in the course of their virtual travels.[14] In fact, most web addresses contain no indication of the nationality of the site.[15]

The Internet is also used to send mail in just a few seconds anywhere in the world. The E-mail permits rapid communication between individuals and makes it easy, using mailing list, to send out the same message to multiple addresses.

The Internet is an extraordinary way of communicating. With the Internet, one can sit in their chair and find quite anything the may be looking for around the world. This is the reason why the Internet, since the beginning of the 1990's, has developed so rapidly. In 1981,

---

[10] A search engine permits, by entering words, to find the related web sites.
E.g., yahoo at http://www.yahoo.com
excite at http://www.excite.com

[11] E.g., www.fedworld.gov/supcourt/index.htm

[12] E.g., http://www.law.cornell.edu; http://law.house.gov

[13] Hypertext describes a document with nonlinear links (or connections) to other parts of the document or other documents.

[14] See Matthew R. Burnstein, Conflicts on the Net: Choice of Law in Transnational Cyberspace, 29 vand. J. Transnat'L. 75, *80 (1996).

[15] Fifty percent of the connection time is devoted to the web.

there were a mere 213 host computers on the Internet. Ten years later, there were 400,000. By 1995 that figure had jumped to 4.8 million.[16]In 1996, over 9.4 million computers were linked on the Net and the number of hookups is growing rapidly. It is estimated that there are 50 million Internet users world-wide, 24 million in North America[17], including 1.1 million children under 18 years of age.[18] These estimates will certainly be outdated even as this thesis is being read. As far as businesses are concerned in the United States alone, fifty new businesses and one thousand new host computers join the Internet every day. France Telecom receives each day more than 1,000 requests for new connections. In January, 1993, there were 1,313,000 providers. In 1996 there were 9,472,000. In Europe, the number of servers[19] increased by 60% over the period January 1995-January 1996. If the Internet was unheard a few years ago, it seems to now be in the news every day. Newsweek magazine declared 1995 the Year of the Internet.[20]

The rapid development of the Internet is also driven by the low cost of using it. When the user connects their computer to the Internet to surf the Web or use E-mail, they pay only a local communication fee, even if they use a site located on the other side of the world. For example, sending a fax from Paris to Los Angeles costs 60 FF ($12) and this operation takes six minutes. E-mail sends the same information for only 1FF (20 cents), and takes just a few seconds.

The Internet offers others advantages. In social terms, it represents significant potential benefits. It offers unprecedented opportunities for empowering citizens, and for connecting them to ever richer sources of digital information. Lowering the barriers of entry

---

[16] G. Burgess Allsion, The Lawyer's Guide to the Internet 19, at 175 (1995).

[17] Kara Swisher, Internet's Reach In Society Grows, Survey Finds; Internet's Popularity Grows with Public, Survey Finds, Wash. Post, Oct. 31, 1995, at A1.

[18] Business News Briefing, Rocky Mountains News, Jan. 12, 1996, at 56 A.

[19] A server is a program or computer that services another program or computer (the client).

[20] Steven Levy, *The Year of the Internet*, NEWSWEEK, Dec. 25, 1995, at 21.

to the dissemination of information on the local, as well as on the global scale, the Internet allows individuals or associations to publish information about their activities to a wide audience at a modest cost. In the field of advertising and marketing, the Internet presents a number of significant and well-documented advantages. Because of its interactive nature, and the immediacy and ease of communication, advertised messages can be targeted at audiences much more precisely than it before, and feedback can be obtained more easily from current or potential customers.

More than this, what also incites somebody to "surf" on the web is his feeling of freedom, he is allowed to go everywhere without any restriction.

More over, as the US market already demonstrates, the Internet is directly fostering a new and fast growing Internet economy, creating new categories of business and new jobs[21].

Internet is also very useful for the lawyer and his client. By the way of the Internet, it is now possible to draft a contract on line, to sell an apartment in Berlin while staying in Atlanta.

The vast majority of Internet content is concerned with information for totally legitimate (and often highly productive) business or private usage. However, like any other communication technology, the Internet carries some potentially harmful and illegal information, and can be misused as a vehicle for criminal activities in a wide range of areas, for example: misappropriation of intellectual property (unauthorized distribution of copyrighted works, e.g., software, writings, music); endangerment of minors (abusive forms of marketing, violent images, pornography); attacks on human rights (propaganda promoting

---

[21] An estimate by Forrester Research concludes that the Internet "core economy" has generated in the US alone some $2.2 billions in 1996. By the year 2000, some $45.5 billions will be directly attributable to the Internet activity. According to Forrester Research, the Internet's most intense economic activity will center on Internet infrastructure ($14.2 billions), consumers content ($2.8 billions, including Internet advertising and rights purchases), business content ($6.9 billions, including business intelligence now supplied on proprietary networks), online trade ($21.9 billions) and financial services (management through the Internet of an estimated $46.2 billions in assets and savings).

racial hatred and discrimination[22]); breaches in national security (instructions of bomb-making, diffusion of secret documents); or publication of prohibited documents. [23]

An example of a problem that may arise occurred in January 1996, in France, a few days after President François Mitterrand died. A book (Le grand secret, *The Big Secret*) was published by a journalist, Mr. Gonod, and the ex-personal physician of the president, Dr. Gübler. In this book, the doctor stated that Mitterrand had known about his cancer since the beginning of his first mandate in 1981, and the doctor disclosed many details about Mitterrand's illness and private life. Mitterrand's family obtained a court order banning the book for violation of privacy rights. Shortly after this order was issued, someone scanned the book and put it on a web server in the name of freedom of expression. A few days later, the web server was closed, but the book had already been reproduced in servers located outside France, including the server of MIT. This illustrates an important problem. Information prohibited in one country may be legal in another[24]. What is considered to be acceptable for posting on the Internet varies between nations and cultures. Every country must define their own borderline between what is permissible and what is not.[25]

Another example of a wrong that has been committed in cyberspace is the dissemination of hate speech and threats.[26] A computer bulletin board operated by the Aryan

---

[22] The Internet has a "dark underside" declared President Clinton after the April 19, 1995 terrorist bombing of a federal building in Oklahoma City. The President was responding to reports that secretive anti-government milita groups were using "the Net" to organize rebellions or spread messages of hate. See Charles S. Clark, *Regulating the Internet*, 5 CQ RESEARCHER, 563, 563 (1995).

[23] Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Illegal and harmful content on the Internet*, (1996). Available at http://www2echo.lu/legal/en/internet/content/communic.html

[24] Another example is the fatwa against Salman Rushdie.

[25] See Valérie Sédaillan, Controlling Illegal Content over the Internet, at http://www.argia.fr/lij/english/control.html.

[26] E.g., officials charged a University of Michigan student with a federal crime for describing the torture and rape of a character named after a female classmate in a message posted to the Usenet newsgroup "alt.sex.stories." USA Today, Feb.10, 1995, at 3A.

Nations Net in the United States promotes white supremacy and maintains a list of targets for extermination. These messages are however illegal in Canada, which prohibits the circulation of literature promoting genocide.[27]

It is the role of the lawyer to find a legal answer to these problems and to define the legal scope of the Internet. Indeed, what is allowed or forbidden on the Internet has not been well outlined. To what extend is it permissible to write or show something on the Web? The current users of the network ask themselves many legal questions that lawyers have to answer: how to protect a writing, how to sue an infringer, who is liable, how to punish offenders and how to enforce judgment, which law is relevant, and whether a law created to regulate content on the Internet is compatible with the constitutional principle of free speech.

Answers to these questions are difficult to discern. However, existing laws regulating information exchange provide some answers. The difficulty is to find which of these laws is relevant to this new mode of exchange, how to apply it and may be how to adapt them to the Internet in order to answer the previous questions and facilitate the legal understanding of the Internet.

This thesis will explain the legal aspects of the Internet, so that users who wish to protect their rights and avoid liability can log on with a better understanding of the rules of the game. This work will be divided in two chapters.

The first chapter will focus on existing legal regulation of the Internet to adivise users on which law is relevant, and how to solve problems of conflicts of laws in the cyberworld. It will answer the question whether cyberspace is, or not, a "no laws land", and what kind of regulation would better fit the cyberworld. This first chapter will also warn users on their potential liability on the Internet, liability of the final user, and of the provider.

---

[27] Anne W. Branscomb, Jurisdictional Qandaries in Global Communications Networks, in Toward a Law of Global Communications Networks 92 (discussing Transnat'l Data Rep., Feb. 1987, at 7).

The second chapter will describe what is the legal utilization of the Internet by users and authors, to warn them, first of all, on where is the limit between normal use of a work and infringement of copyright, and second of all, on what kind of speech they are allowed to load. The Internet raises, indeed, many problem of copyright infringement (is the work loaded on the network protected, how to enforce the exclusive rights?), but also many questions relative to the principle of Freedom of Speech (what about pornography on the Net, or any kind of extreme speech?).

After having answered all these questions, this work will conclude, that Governments should respect the initial goal of the Internet -a free flow of information-, and not try to muzzle it with inadapted regulation. The users of the Internet are the best placed to organize a regulation that will best fit this new medium, and great, medium of expression.

CHAPTER I

REGULATION OF THE INTERNET

Someone is in front of his computer, connected to the network and ready to enter for the first time the vast world of the Internet. He wants to use all the capacities of this new way of communicating, and not only surf on the Web and send E-mail, but also creates his own Web site and sends his own information all over the world.

But this person must take care that before pushing the "start button", he knows where he is going and what the legal ramifications of this voyage are. This knowledge may avoid missteps and liability.

Indeed, when one is connected to the Internet it is as if he was in a car on the highway[28]. If he knows how to control his car and all the practical aspects of driving, but does not know the code, the rules of driving, he will not go far before making mistakes with heavy consequences.

This first part of this chapter will deal with the legal scope of the Internet and describe the rules which govern the electronic superhighway, so as to help the user avoiding mistakes. The second part of this chapter will describe the consequences if these rules are not respected and are infringed upon, how those responsible will be searched out and liability ascertained.

---

[28] Information superhighway is another name for the Internet.

FIRST PART: THE RELEVANT RULES

The Internet is a "global village"[29] encompassing every country. Each country applies its own laws to the network. That means that one should know the laws of approximately one hundred and ninety countries to surf safely on the Web.

This work will be restricted to the study of the US law (the US being the most advanced country in the utilization and exploitation of the network), with some analysis of European and French law. Since different laws and rules apply in different countries to the same subject, conflicts of law are inevitable, and will be elaborated upon.

I] Positive law (rationae materiae)[30]

The purpose of this section is to advise the reader on the general and the specific rules that govern the Internet.

Four major sources of law, apply to the Internet just as to any other domain of law: The Constitution (1), treaties (2), statutes (3), the contracts (4).

A) The US Constitution and Conventions

The first, and certainly the most important, principle governing the Internet is the freedom of expression outlined in the First Amendment of the US Constitution[31] and in

---

[29] University of Toronto professor Marshall McLuhan coined the term "global village" in the 1960's. See supra footnote1.

[30] This section will not deal with the copyright law, will be studied separately in Chapter II, as copyright is a central issue in the study of the legal aspects of the Internet.

[31] U.S. CONST. amend. I.

article 11 of the French Human Rights Declaration of 1789[32]. All regulation of material transmitted through the medium of interactive communication is subject to this privilege.

The First Amendment provides in relevant part "Congress shall make no law (...) abridging the freedom of speech, or of the press (...)."[33] The aim of the framers of the Constitution when they drafted this Amendment was to ensure the continual free exchange of political ideas and social sentiment.[34] The first Continental Congress stated that:

> "The importance of this [freedom of speech] consists, besides the advancement of truth, science, morality, and arts in general, in its diffusion of liberal sentiments on the administration of Government, its ready communication of thoughts between subjects, and its consequential promotion of union among them, whereby oppressive officers are shamed or intimidated, into more honorable and just modes of conducting affairs."[35]

Justice Holmes further defined the rationale for protecting freedom of expression as ensuring "free trade in ideas" stressing that society must have access to all opinions, favorable or unfavorable, to permit individuals to make informal choices.[36]

The First Amendment, defined broadly, applies in a great number of online legal situations and assures that all users of online systems can communicate freely with one

---

[32] Déclaration des Droits de l'Homme et du Citoyen. Art. 11. "The free communications of thoughs and opinions is one of the most precious rights of Man. Any citizen may thus freely speak, write, print, except where he abuses this freedom in cases determined by the law."

[33] The First Amendment provides:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

[34] Roth v. United States, 354 U.S. 476, 484 (1957).

[35] Id. at 484 (citing 1 Journals of the Continental Congress 108 (1774)).

[36] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. Dissenting).

another. The First Amendment is the primary source of rights and protection of travelers on the information superhighway.[37]

The second important constitutional principle governing the Internet is found in the Fourth Amendment, which provides "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures (...)"[38] This amendment affirms therefore the right of privacy, and the right of freedom from intrusion by strangers, for example in the exchange of Electronic-mail.

Some international Conventions are also relevant to the insuring of the free flow of information on the Internet. The Universal Declaration of Human Rights, adopted December 10, 1948 [39], states in article 19, "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."

This philosophy was taken from the French Declaration of Human and Citizen Rights of 1789 [40], which also inspired Article 10 on Freedom of Speech of the European Convention on Saveguarding Human Rights and Fundamental Liberties[41].

B) The treaties

One hundred and sixty nations met in December 1996 to consider revisions to international copyright laws. They enacted two new international treaties protecting

---

[37] Cauesaway Medical Suite v. P.Ieyoub, 1997 WL 142113 (5th Cir. (La) 1997).
"No one would dispute that the First Amendment protects television or the Internet, (..) even though non of these technologies existed in the late eighteenth century."

[38] US. CONST. Amend IV.

[39] Universal Declaration of Human Rights, Adopted by United Nations General Assembly Resolution 217A (III) of December 10, 1948.

[40] Déclaration des Droits de l'Homme et du Citoyen (1789).

[41] Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales.

intellectual property in the digital age. One treaty deals with the protection of literary and artistic works [42], and the other with music recordings and phonograms[43] . Once these treaties are ratified by all one hundred and sixty nations, authors of musical, artistic, and literary works will be able to be paid for work they make available on the Web.[44]

C) Statutes

US and French statutes most relevant to the Internet will be discussed.

1) United States Statutes

There are five specific US statutes directly relevant to the Internet[45]: the Computer Fraud and Abuse Act of 1984[46], (amended five times, lastly in 1994), the Electronic Communications Privacy Act (ECPA) of 1986 [47], the Communications Assistance for Law Enforcement Act (CALEA) of 1994 [48], the Digital Performance Right in Sound Recordings

---

[42] Diplomatic Conference on Certain Copyright Neighboring Rights Questions: World Intellectual Property Organization (WIPO) Copyright Treaty adopted December 20, 1996.

[43] Performance and Phonogram Treaty, World International Property Organization, December 20, 1996.

[44] These two treaties may be viewed at http://www.wipo.int:80/

[45] A proposition of Act about the privacy on the Internet has been introduced in the House of Representatives January 7, 1997: Consumer Internet Privacy Protection Act of 1997, 105th Congress, 1st Session, H.R. 98.
The aim of this Act is to regulate the use by interactive computer services of personally identifiable information provided by subscribers to such devices.

[46] 18 U.S.C. s 1030 (West Supp. 1996).

[47] 18 U.S.C. ss 2510-2521 (1994).

[48] Pub. L. No. 103-414, s 101, 108 Stat. 4279 (1994) (codified as 47 U.S.C. s 1001 et seq. (1994)).

Act of 1995[49], and the Telecommunications Act (Telecom Act) of 1996[50] . They will be studied in this order the one after the other.

The Computer Fraud and Abuse Act describes six offenses[51]. Those that apply to Internet users will be described below[52].

The first offense involves unauthorized access to national defense, foreign relations, or other restricted data, as defined in the Atomic Energy Act[53]. This offense is not easy to prosecute, however, because the prosecutor has to proved that the hacker[54] intended to use the restricted information to injure the United States or to aid a foreign nation.

The third offense involves access to computers used exclusively by or for the Government of the United States, and more specifically, involves access which affects the functioning of those computers. An Internet user was charged in a recent case with this offense because his unauthorized access affected the operation of Government computers[55].

---

[49] It amends 17 USC § 101 & 106.

[50] Telecommunications Act of Feb. 8, 1996, Pub. L. No 104-104, 1996 U.S.C.C.A.N. (110 Stat. 56) 133, 134 (to be codified at 47 U.S.C. s 223).

[51] *Unauthorized Access to National Defense, Foreign relations, or restricted area; 18 U.S.C. s 1030(a)(1).

* Unauthorized Access to Financial Records; 18 U.S.C. s 1030(a)(2) (does not apply to the Internet).

* Access Affects Use; 18 U.S.C. s 1030(a)(3).

* Computer Fraud 18 U.S.C. s 1030(e)(2).

* Alters, Damages, or Destroys Information; 18 U.S.C. s 1030(a)(5).

* Trafficking Passwords; 18 U.S.C. s 1030(a)(6).

[52] It the case of the first, the third, the fifth and the sixth.

[53] 42 U.S.C. s 2104(y).

[54] A hacker is a computer pirate who violates computer privacy by intercepting and possibly using telephone and credit card numbers, reading electronic mail, or by taping into sensitive government databases.

[55] United-States v. Morris, 928 F.2d 504 (2d Circ. 1991).

The Act also criminalizes accessing a federal interest computer[56] with the intent to defraud and obtain something of value (other than computer time). Fraud is therefore covered by this section.

The fifth offense involves knowingly or recklessly altering, damaging or destroying information. This section includes "any computer used in interstate commerce or communication". Since any computer accessing the Internet is engaged in interstate communication, any intentional access without authorization which alters, damages, or destroys information constitutes a crime.

The sixth offense deals with trafficking passwords, and applies to any Internet computer, as long as it could be shown that such trafficking affects interstate or foreign commerce, or is used by the U.S. Government.

The ECPA is the privacy shield protecting e-mail. The statute provides in part that "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication" shall be fined or imprisoned.[57] In essence, this law prohibits anyone but the sender or the intended recipient from reading an intercepted e-mail message.

The CALEA expands privacy protection for telephone and computer communications, including protection of E-mail addresses. A proposition bill about the privacy and the Internet has been introduced in the House of Representatives January 7, 1997. It intents to create a Consumer Internet Privacy Protection Act. The purpose of this Act

---

[56] A "federal interest computer" is defined as a computer :

(A) exclusively for the use of a financial institution or the United-States Government, or in the case of a computer not exclusively for such use, used by or for a financial institution or the United-States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same state.

18 U.S.C. 1030(e)(2)

[57] 18 U.S.C. § 2511 (1)(a) and (4).

would be "to regulate the use by interactive computer services of personally identifiable information provided by subscribers to such services".[58]

The Digital Performance Right Act grants copyright owners of sound recordings the right to authorize digital transmission of their works. The Act amends 17 U.S.C. § 106 (6) so that the owner of a copyright has the exclusive right "in the case of a sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission" [59].

In 1934 the Communication Decency Act (CDA) was enacted, prohibiting "indecent and obscene interstate commercial telephone messages". It was designed to restrict "the access of minors to 'dial-a-porn' services".[60]

The CDA was amended in February 1996 to protect children from the viewing of sexually and indecent adult-oriented web sites[61]. The revised CDA and the Internet Freedom and Family Empowerment Act (the Cox/Wyden Amendment) together constitute the Telecommunication Act[62] (Telecom Act). Senator James Exxon of Nebraska submitted an amendment to section 223 of Tittle 47 of the CDA, which substitutes the phrase "telecommunication device" for the word "telephone", thereby expanding the language of the statute to encompass communication by computer. Under this new legislation, anyone who knowingly facilitates any form of "obscene, lewd, lascivious, filthy, or indecent"[63]

---

[58] This bill may be viewed at http://www.epic.org/privacy/internet/hr_98.html

[59] 17 U.S.C 106 (6).

[60] 47 U.S.C. § 223(b).

[61] According to Senator Exxon, "this will protect children from exposure to indecent material with the least amount of inconvenience to adult users".
Telephone Interview with Russ Rader, Press secretary for Senator Exxon (Sept 15, 1995).

[62] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56.

[63] 47 U.S.C. § 223 (a).

communication by way of any telecommunication device is subject to prosecution.[64] However, many commentators of this Act criticized it, assuming that it is unconstitutional. The United States District Court of Pennsylvania, in *American Civil Liberties Union v. Reno* [65] held that this Act is unconstitutional by violating the First Amendment of the constitution.[66]

The CDA grants a consultative role to the Federal Communications Commission (FFC)[67] to "describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications"[68]. However, the FCC is granted no enforcement authority over such measures.

The Internet Freedom and Family Empowerment Act states the commitment of the United States to promoting the development of the Internet, to preserving the "vibrant and competitive free market"[69] that exists, "unfettered by Federal or State regulation"[70] , to

---

[64] 47 U.S.C. § 223(a) provides: (a) Whoever - (1) in the District of Columbia or in interstate or foreign communications (A) by means of telecommunications device knowingly - (I) makes, creates, or solicits, and (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person; ... or (2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity shall be fined under Title 18 [not more than $100,000] or imprisoned not more than two years, or both.

47 U.S.C. 223(d) provides: whoever - (1) knowingly within the United-States or in foreign communications with the United-States by means of telecommunications device makes or makes available any obscene communication in any form including any comment, request, suggestion, proposal, or image regardless of wether the maker of such communication placed the call or initiated the communications; or (2) knowingly permits any telecommunications facility under his control to be used for any activity, shall be fined under Title 18 [not more than $100,000] or imprisoned not more than two years, or both.

[65] 929 F. Supp. 824 (1996). See also Shea v. Reno, 930 F. Supp 916 (1996).

[66] The case is now in front of the United States Supreme Court. See Chapter II Second part.

[67] Created by the Communication Act of 1934, ch. 652, § 151.

[68] 47 U.S.C.A. § 502 (2)(e)(6).

[69] 47 U.S.C.A. § 230 (b)(2).

[70] Id.

encouraging the development of technologies to maximize user control over available information, and to ensuring vigorous enforcement of the laws to "deter and punish trafficking in obscenity, stalking, and harassment by means of computer".[71] More over, the Cox/Wyden Amendment creates a "good Samaritan" exception, to protect innocent access providers.[72]

The aim of the Telecom Act is to give law enforcement new tools to prosecute those who would use a computer to make the equivalent of obscene telephone calls, to prevent the electronic distribution of obscene materials, and to improve the powers of prosecution of those who would provide pornography to children via computer[73].

The Telecom Act makes adult access codes, and adult personal identification numbers mandatory to gain access to sexually-oriented user groups[74]. The pass codes will be distributed only to those who show proof of age, by their mailing in age verification forms or by their using of a credit cards.

Finally, the Telecom Act preempts any state or local regulations inconsistent with its definition of liability.[75] However, as will be seen, some states have enacted their own Internet legislation.

Other laws have also been enacted to further outlaw the inappropriate use, which deviates from the initial purpose of the Internet. For example, the senate passed by, the way of the Department of Defense Authorization Act for Fiscal Year 1997, section 1088 entitled: "Prohibition on the distribution of information relating to explosive materials for a criminal

---

[71] 47 U.S.C.A. § 230 (b)(5).

[72] 47 U.S.C.A. § 230 (c).

[73] Dominic Andreano, Cyberspace: How Decent is the Decency Act?, 8 St. Thomas L. Rev. 593 (1996).

[74] See 47 U.S.C.A § 223(e)(5)(B).

[75] 47 U.S.C.A. §223(f)(2).

purpose"[76]. This section provides in its relevant part that " it shall be unlawful for any person to teach or demonstrate the making of explosive materials, or to distribute by any means of information (...) The manufacture of explosive materials (...)". The state of Georgia enacted a similar statute prohibiting the computer transmission of bomb-making instructions.[77]

Many state have enacted their own Internet legislation. The "Georgia Computer Systems Protection Act" was signed into law on April 18 and took effect July 1. 1996. It makes it a misdemeanor to knowingly use another's "individual name, trade name, registered trademark, logo, legal or official seal or copyrighted symbol to falsely identify the person" to send the data on a World Wide Web homepage or mailbox site.[78] This Act also precludes the use of pseudonyms by Internet users.

In the area of Child Pornography, the Commonwealth of Virginia enacted Senate Bill No. 1067[79] on May 5, 1995, which expands the definition of sexually explicit visual material to include child pornography distributed through the Internet. The term 'sexually explicit materials' now includes pornographic digital images of children.[80]

Regarding electronic transmissions of works, a bill, the National Information Infrastructure Copyright Protection Act is currently pending in both the House of Representatives and Senate.[81] This Act is the legislative result of the proposed legislation included in a government White Paper introduced in the Congress in 1995. This White Paper has been recommended by the Working Group on Intellectual Property Rights, a committee set up by the Clinton Administration to propose changes to copyright law and promote the

---

[76] Enacted at: 18 U.S.C. § 842.

[77] 1995 Ga. Laws 322. This law was enacted on April 12, 1995 and expands the definition of "communication facilities" to include a computer or computer network.

[78] Georgia H.B. 1630 SN.

[79] 1995 Va. Acts 839.

[80] VA. CODE. ANN. § 18.2-374.1(A).

[81] H.R. 2441 104th Congress, 1st Sess. (1995), S. 1284, 104th Cong., 1st Sess. (1995).

development of the NII. This task force recommends that Section 106(3) of the Copyright Act be clarified to expressly recognize that copies or phonorecords of works can be distributed to the public by transmission, and that such transmissions fall within the exclusive distribution right of a copyright owner.[82]

The laws governing the Internet in the United States have been presented. We will now take a quick look at French and European laws dealing with the Internet.

2) French and European statutes

On July 21, 1996, the Law for Regulation of Telecommunications[83] was enacted in France to regulate specifically the Internet. This rule includes an amendment (article 43-2 and 43-3) of the law of September 30, 1986[84] on audiovisual broadcast. This amendment is a regulation of the Internet. According to this law, an Internet Service Provider (ISP) is a broadcast service, which require prior authorization by the CSA (Superior Audiovisual Counsel), an independent authority which control broadcast. If it is authorized to exercise, the ISP must propose to its client a technical device to enable them to block access to certain services and to select them. The CSA was to adopt certain guidelines to ensure the respect, by audiovisual Internet services, of ethical rules[85] adapted to the nature of these services. These recommendations are published on the Official Journal.[86] There is also a committee assigned to evaluate the compliance of Internet services with the recommendations. When

---

[82] Issues dealing with copyright law will be studied in the first part of the second chapter of this thesis.

[83] Loi n° 96-659 du 26 juillet 1996 de Réglementation des Télécommunications.

[84] Law N°86-1067 of September 30, 1986.

[85] E.g., incitement to racism hatred, negationist speech.

[86] The Official Journal publishes all French laws and regulations.

development of the NII. This task force recommends that Section 106(3) of the Copyright Act be clarified to expressly recognize that copies or phonorecords of works can be distributed to the public by transmission, and that such transmissions fall within the exclusive distribution right of a copyright owner.[82]

The laws governing the Internet in the United States have been presented. We will now take a quick look at French and European laws dealing with the Internet.

2) French and European statutes

On July 21, 1996, the Law for Regulation of Telecommunications[83] was enacted in France to regulate specifically the Internet. This rule includes an amendment (article 43-2 and 43-3) of the law of September 30, 1986[84] on audiovisual broadcast. This amendment is a regulation of the Internet. According to this law, an Internet Service Provider (ISP) is a broadcast service, which require prior authorization by the CSA (Superior Audiovisual Counsel), an independent authority which control broadcast. If it is authorized to exercise, the ISP must propose to its client a technical device to enable them to block access to certain services and to select them. The CSA was to adopt certain guidelines to ensure the respect, by audiovisual Internet services, of ethical rules[85] adapted to the nature of these services. These recommendations are published on the Official Journal.[86] There is also a committee assigned to evaluate the compliance of Internet services with the recommendations. When

---

[82] Issues dealing with copyright law will be studied in the first part of the second chapter of this thesis.

[83] Loi n° 96-659 du 26 juillet 1996 de Réglementation des Télécommunications.

[84] Law N°86-1067 of September 30, 1986.

[85] E.g., incitement to racism hatred, negationist speech.

[86] The Official Journal publishes all French laws and regulations.

the committee decides that a service does not abide by these guidelines, their findings are published on the Official Journal, and the interested parties are notified directly by the CSA.

A group of senators asked the French Constitutional Council to examine the law for compliance with the French Constitution. It has found articles 43-2 and 43-3 unconstitutional, because contrary to the freedom of speech as stated in article 11 of Human Rights Declaration of 1789, which has constitutional value.[87]

Another law, not specially enacted to regulate the Internet, but which contains articles relevant to it has been applied to the Internet in France: the Law on the Use of French language[88] and its application decree.[89] It has been enacted to forbid the use of English words in the French language, and to prevent English from being the language of news technologies.

France has also proposed to the countries belonging to the OECD an International Cooperation Treaty on the Internet, which would establish a common commitment to the protection of copyright, juridical cooperation, and respect of deontological principles.[90]

These are the relevant rules applicable to the Internet. It is also possible to regulate the Internet by the way of the contract.

D) Contract Law

Contracts fill the so-called "no law's land" where no statutory law clarifies business relations between people. Contracts are everywhere when dealing with the Internet. There

---

[87] Decision n°96-378 DC of July 23rd, 1996, JO July 27, 1996.

[88] Loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française.

[89] Décret d'application n° 95-240 du 3 mars 1995.

[90] France proposed also with its Telecommunication Act a similar treaty binding French or people putting messages at the destination of France. It is possible to read this Treaty at: http://www.planete.net/code-internet

is a contract between the provider, server, and the user, for example for an individual to open a web site, a contract with the provider is required. More over, when surfing the Web, one may reach sites that require agreement with certain conditions before entering[91]. Many contractual links exist between the different actors of the Internet. Access to Prodigy, Compuserve, America Online[92] is already subject to contractual agreements. Users must go through some form of initial "sign-on" procedure, whether on-line or by paper transaction, by which they identify themselves, agree to make payments, agree to abide by whatever rules the system administrator imposes, etc. At that point of entry, the controlling system administrator can require adherence to a contract that specifies "legal" and "illegal" behavior. An example taken in the scope of the e-mail will clarify this point. Besides reading and writing e-mail, many users also rely on the ease of copying already digitized messages to forward copies of such messages to others who might find them of interest. Written messages are copyrighted.[93] Users who forward others' messages are reproducing and distributing copyrighted materials in violation of the copyrighted laws. In such a case, the contract will be very helpful to solve this problem. This solution has already been chosen by Lexis Counsel Connect, which is a large service provider. Subscribers to this service sign an initial contract whereby they grant the right of reproduction of their messages to others. Therefore, the contract resolves the tension between frequent practice and copyright law.[94]

---

[91] It is for example the case for the adult reserved site: one is allowed to enter the site only if one is over 21 years of age and if one is not in a state that prohibits such viewing.

[92] They are Bulletin Board System: It is a computer system to which other computers can connect, so their users can read and leave messages or retrieve and leave files.

[93] See Chapter II, First part.

[94] These are the different links governing all the Internet actors:

User1
Telecom — Access / service provider — Server — Author
User2

Contracts also allow all parties involved to choose the law applicable to their situation, and then avoid problems of conflicts of law which can occur quite often because of the international nature of the Internet. The law of a given country applies up to the limit of sovereignty of that country, and sovereignty has traditionally been a function of physical territory. The Internet is not reconcilable with this paradigm. The Internet crosses political borders and, in doing so, causes the user to travel through vastly different legal climates. Conflicts of laws across borders becomes a very complicated issue which contracts can reduce.

II] Conflicts of laws

The purpose of this part is to provide to relevant legal information to victims of an Internet actors.

A) Which juridical problems may arise on the Internet?

Traditional notions of jurisdiction are outdated in a world divided not into nations, states, and provinces, but networks, domains, and hosts. Cyberspace confounds the conventional law of territorial jurisdiction and national borders. In cyberspace, it does not matter at all whether a site lies in one country or another because the networked world is not organized in such fashion. Telnet [95], gopher [96], and the World Wide Web all render political

---

[95] Telnet allows users to "log-on" to a remote host computer as if they were sitting in front that computer.

[96] Gopher is a menu-based way to navigate the Internet by allowing the users to quickly access information elsewhere and download that information to their own computer.

borders, to some extent obsolete [97]. Frequently, users are unaware that they have even "crossed" a political border in the course of their virtual travels.

When litigation arises from activity in a transnational cyberspace, whose laws apply? Private international law is concerned exclusively with private disputes between individuals (or analogous entities like corporations), while public international law addresses issues such as state recognition, treaties and war. The multistate nature of cyberspace highlights the importance of conflict of law questions in international civil litigation arising from Internet participation[98].

The substantive legal regulations of what country apply to a defamatory message that is written by someone in Columbia, read by someone in Australia by means of an Internet server located in the United States, injuring the reputation of an English person? Whose courts have jurisdiction over adjucation of claims of injury or violation of national laws? Must the English person go for legal redress to Bogota or to the United States to find a legal institution with power over either of the two potential guilty parties? If not, and if jurisdiction exists in England, the most convenient forum for the victim, how is a favorable decision by an English tribunal, ordering that the Columbian originator or the American intermediary pay damages to be enforced outside of England?

Similar questions exist in a criminal context. Suppose the message is criminal instead of defamatory, involving child pornography or indecency, or involving financial fraud, forgery or terrorism. Must the wrongdoer be tried only where he or she is physically located? If the answer is no, how is the wrongdoer to be appended and extradited to the place where judgement is to be served? Whose substantive criminal law should apply?

---

[97] A web site at the University of Kansas allows a user to "spin" a graphical roulette wheel and then be "transported" to the site in any state or country on which the pointer lands. Available on the web at http://kuhttp.cc.ukans.edu/cwis/organizations/kucia/uroulette.html

[98] "Choice of law is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty." Dan L. Burk, Patents in Cyberspace, 68 Tul. L. Rev. 1, 5 (1993).

B) Where can a cyberspace user[99] be subject to suit?

In order to answer this question in the specific field of the Internet, one must refer to the rules that apply to transnational litigation in general. The main objectives of choice of law are to achieve "maximum fairness to the parties" and to achieve "effective implementation and coordination of state or country policies"[100]. The most common disputes which will arise in the scope of the Internet, are disputes involving the enforcement of contracts and tort cases.

Historically, choice of law was driven by formal rules such as lex loci contractu, which required the application of the substantive law of the place of contracting in the case of a contract dispute, and lex loci delicti in the case of an action in tort.[101]

In the case of a contractual dispute over the Internet, it will be easy to determine the relevant law if a forum has been preapproved by the parties. Without a contractual forum selection clause, the choice of law defers to the law of that nation most closely connected with the relevant contractual issue. The place of contracting refers to the State which has the most significant relationship to the transaction and the parties. Thus, if a dispute arises over the formulation of a contract, the law of the nation in which the contract was made, or negotiated would likely apply. If the dispute is performance related, the applicable law is that of the place where the performance was to occur, or where the subject matter of the contract is located.[102] In the case of a tort action -for example defamation-, different possibilities exist to find the forum. It could be: any State in which the offending material or message was

---

[99] The term user is here employed in its general meaning and encompasses everyone, individual or not, who may have a link, or a relation with the Internet: provider, server, surfer, author, etc.

[100] George A. Zaphiriou, *Basis of the Conflict of Laws: fairness and Effectiveness*, 10 Geo. Mason U.L. Rev. 303 (1988).

[101] See Restatement (First) of the Conflict of Laws § 377 (1934), and e.g., Joseph Story, Commentaries on the Conflict of Laws ch. XIV (4th Edition 1852).

[102] 10 Geo. Mason U.L. Rev. at 316.

assertion satisfies due process.[107] When a forum seeks to establish jurisdiction over a nonresident, courts employ a "minimum contacts" test.[108] The activity of the nonresident must be such that the defendant should have "reasonably anticipate[d] being haled into court"[109] in that forum.

In the case of the Internet, there is an added level of complexity, as it is possible for users to post messages, articles, pictures and other materials to be read or watched and downloaded by users in other countries. Are these messages "purposefully directed" toward the forum country? This would be difficult to ascertain as the defendant will argue that much of cyberspace activity is not purposefully directed toward any given country.[110] It will therefore, not be easy for a plaintiff to prove the required minimum contacts between the defendant and one or another jurisdiction.

U.S. courts have, nevertheless, already had to answer this kind of problem of choice of forum in cases involving two differents states. For example, the United States District Court from the District of Connecticut[111] held in a case involving a Connecticut plaintiff and a Louisiana defendant that:

> "Non resident's transmision of fraudulent misrepresentations to resident by telephone, electronic mail, and on-line computer service talk forum constituted 'tortious act within the state'; and therefore nonresidents's actions were within Connecticut long-arm statute, telephone call and electronic messages to resident

---

[107] Northrup King Co. V. Compania Productora Semillas Algodoneras Selectas, SA., 51 F.3d 1383, 1387 (8th Cir. 1995).

[108] International Shoe Co. V. Washington, 326 U.S. 310, 316 (1945).

[109] World-Wide Volkswagen Corp. V. Woodson, 4444 U.S. 286, 297 (1980).

[110] For example on a traditional letter the address, with the name of the country is written. An E-mail message does not include a destination state in its address. It is difficult to know that the recipient of a message sent at cnn.feedback@cnn.com resides in Georgia U.S.

[111] Cody v. Ward, 954 F. Supp. 43 (1997).

established sufficient minimum contacts; and exercise of personal jurisdiction over nonresident was fair under due process clause."[112]

In a case involving parties from two differents countries (United States and Italia), the United States District Court from the South District of New York[113] determined whether the defendant distributed or sold his magazine (Playmen) in the United States (forbidden by a prior injunction agreed to after a suit by Playboy, Inc.) when it established an Internet site containing this magazine. The defendant argued that the court had neither personal nor subject matter jurisdiction to determine the issue raised. The Italian corporation claimed it had no agent of office within the United States and that it did not publish, distribute or sell its magazine in the U.S. The court just answered: "this Court retained jurisdiction over defendnat for purposes of enforcing the 1981 injunction".[114]

It may appears upon reading this, that the choice of law is always determined by the place and location of certain events. It has been said that the Internet confounds notions of place and location. Relying on the place of contracting, or the place of performance, leads to the conclusion that place and location mean little or nothing when it comes to Internet contracts. In transnational cyberspace, the place and the location might be any of the 190 nations that are on-line. If a contract between a commercial Internet provider and a newsgroup manager is formed in cyberspace, payment is electronically made in cyberspace, and performance is accomplished by services rendered in cyberspace. In the case of tort action, if injury occurs in cyberspace, where the wrong has been committed is Cyberspace itself. It is therefore often not possible to define with certainty the real 'crime scene'.

By nature, the Internet confounds notions of place and location. Therefore, the law of the country which has the most significant relationship to the dispute is the best or at least

---

[112] Id. at 43.

[113] Playboy Enterprises, Inc., v Chuckleberry Publishing, Inc., 939 F. Supp. 1032 (1996).

[114] Id. at 1036.

the less bad choice. Here, the choice of law results not from an arbitrary default rule, but from a careful balancing of all relevant consideration regarding fairness, efficiency, conflicting needs, predictability, parties' expectations, domiciles, policies, and interests in the States involved. Finding the relevant law in a world without any concrete material will lead the plaintiff to link to what he knows, to the only materials he can concretely apprehend. That will be the law of his own domiciles, or of the domiciles of the defendant.

Matthew R. Burnstein noticed however that these rules "do little to solve the choice of law problems in cyberspace, especially when the factors relied upon are geared toward and suited for a real-space world of easily drawn political boundaries."[115] He follows Professor Hardy's[116] idea and proposes instead to apply the Law Merchant [117]to cyberspace. Indeed, lex mercatoria dispenses with the choice of law issues and their attendant balancing and weighing of interests. It makes no attempt to displace existing rules promulgated by the jurisdiction in which a given trade fair might be held. The laws of the interested nations are then displaced by the laws of a collection of merchants (here users) with their own customs and usages of trade. These customary practices inured to the benefit of merchants and were reasonably uniform across all the jurisdictions involved in the trade fairs. As the merchants knew the customs and usages in the lex mercatoria, so too should cyberspace's users be charges with a knowledge of the customs and usage in the on-line world. The interest of this law for the Internet is also that it has the ability to respond and adapt rapidly to changes in technical and legal environments.

---

[115] Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 Vand. J. Transnat'l L. 96 (1996).

[116] I. Trotter. Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U.Pitt. L. Rev 993, 1052 (1994).

[117] The Law Merchant -medieval lex mercatoria- was a collection of customary practices among traveling merchants in Medieval Europe and Asia that was enforceable in all the commercial countries of the civilized world. It was a response to the needs of international commerce.

Burnstein concludes that law would be a collection of selected customs and accepted practices -codified or not- that have developed with cyberspace.[118]

Cyberlaw could therefore evolve from customary precedents. Federal courts could enforce common Internet practice as cyberlaw. The development of such a cyberlaw founds on customs could also lead to the creation of special courts (cybercourts) as Professor Hardy[119] suggests. However, the interest of the Internet is to be a "free" and quick way of communication, not bound by a whole of complicated and heavy rules. The creation of a new jurisdiction is against the essence and aim of the Internet.

C) Enforcement of a judgment

As explained above, because of its nature, the Internet gives rise to several interesting problems even when a dispute and a resulting judgment are entirely local. The problem of turning a judgment into liquid assets becomes even more difficult when the judgment refers to another country.

An author in France may obtain a judgment in a French court for copyright infringement resulting from an act by the operator of an Internet server in Massachusetts. In order to obtain monetary redress, the author must enforce the French judgment involving assets of the server operator in Massachusetts. In such a case, the first step is to obtain recognition of the judgment.[120] Statutory law, such as the Uniform Recognition Act, enacted

---

[118] This is also the point of view of Professor Perrit in:Henry H. Perrit, Jr., *Jurisdiction in Cyberspace*, 41 Vill. L. Rev. 1, 103 (1996).

[119] 55 U.Pitt. L. Rev, at 1052.

[120] When the dispute occurs within the United-States, between persons from different states, the Full Faith and Credit Clause of the United-States Constitution obligates to recognize it.

in about half the states[121], or comity[122], prescribes the criteria for recognition. The courts must recognize foreign judgments unless the party opposing recognition of the judgement can show violation of procedural due process or lack of personal jurisdiction by the rendering foreign court.

The doctrine of comity has been summarized in the Restatement provision: "A valid judgment rendered in a foreign nation after a fair trial in a contested proceeding will be recognized in the United States so far as the immediate parties and the underlying cause of action are concerned" [123].

The Uniform Recognition Act applies to "any foreign judgment that is final and conclusive and enforceable where rendered even though an appeal therefrom is pending or it is subject to appeal" [124].

The enforcement of judgment within the European Community is governed by the Brussels Convention[125] and the Lugano Convention [126], which provide for recognition without any special procedures such as the Deibazione in Italy or the Exequatur in France, Belgium and Luxembourg.

---

[121] Unif. Foreign Money-Judgments Recognition Act, 13 U.L.A. 261 (1962) [hereinafter Uniform Recognition Act]

[122] See de la Mata v. American Life Ins. Co., 771 F. Supp. 1375 (D. Del. 1991) (discussing comity).

[123] Restatement (second) of Conflict of Laws s 98 (1971).

[124] Uniform Recognition Act, supra note 121.

[125] Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial matters, Sept. 27, 1968, 1968 O.J. (L 299) 32, reprinted in 29 I.L.M. 1413 (1990).

[126] Lugano Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, Sept, 16, 1988, 1988 O.J. (L 319) 1, reprinted in 28 I.L.M. 620 (1989).

On paper, it appears to be easy to enforce the judgment of a court of an other country and then recover money, or force someone in an other country to close aweb site. This can work when the involved countries are democratic or develop political links.[127]

One way to ensure the application of the law and the enforcement of a judgement against a foreigner who eludes punishment is the recourse of arbitration tribunal[128]. "The best means for reducing uncertainty with respect to personal jurisdiction, choice of law and venue in civil cases is to use international arbitration"[129]. The use of an arbitration tribunal depends upon the existence of an arbitration agreement, either entered into in advance and involving a class of disputes, or entered into after a particular dispute has arisen and involving only limited that dispute. The power of the arbitrator is therefore contractual and parties are obligated to obey arbitration awards. Arbitration fits well to the context of the Internet. Indeed, arbitrators are chosen by the parties and arbitration procedures and choices of law are specified in the arbitration agreement. In this agreement, it is also possible to state the different remedies, even punitive damages that may be applied. More over, the New York Arbitration Convention provides greater certainty of the enforcement of international arbitration awards than is provided by regular courts. Given the transnational character of transactions on the Internet, this is a great advantage.

For all of these reasons, arbitration is a good way to resolve disputes on the Internet, particularly for the United States, which is not signatory to any treaty that provides for enforcement of civil money judgment across international boundaries. Most of the developed countries, including the US are signatories to the New York Convention[130], which provides that the courts of the signatories are obligated to enforce international arbitration with few

---

[127] See infra page 36.

[128] See Henry H. Perrit, Jr, *Jurisdiction in Cyberspace*, 41 Vill. L. Rev. 1, 93 (1996).

[129] Id.

[130] E.g., France, United Kingdom, Canada, Germany, Japan.

possibilities of refusal. Thus, parties to international cyberspace transactions can greatly increase the certainty of dispute resolution by entering into an international arbitration agreement.

Of course, to utilize such recourse, parties must be willing to enter into arbitration agreements, otherwise the recourse for redress is traditional jurisdiction, with all its limitations. More over, if a party disagrees to apply the award, the only possibility for the plaintiff is to bring the one who does not want to execute in front of a regular court, with all the difficulties that means.

If the recourse of arbitration is a good way to apply the law in cyberspace, it may nevertheless fail. For this reason also, the law merchant is again a good recourse. Users themselves should control enforcement (and remedies). Enforcement of the law established by the customs should be organized and applied by users who would therefore follow an "ethic code" or the "cyberethic".

If, on the paper, it is possible to define all of the regulations that one may use to seek remedies against someone who has infringed upon ones rights or to stop an ongoing infringement, in practice it is not so simple.

Because of the transnational nature of the Internet, remedies must often be sought at the international level, but what can legally and practically be done against an infringer on the Internet? For example, in the Gubler affair[131], what can be done to the MIT server that scanned the prohibited book and put it on the Internet? This book was not forbidden in the United States, only in France. It is not possible for a French court to prevent an American server from sending through the Internet, and here throughout the world, messages which are permitted in the server's own country. The French person could not, therefore, be prevented from reading the forbidden book from his computer in France. More over, if the law forbids an action by sanctioning it, the infringer has to be found. One could think that it is very easy,

---

[131] See introduction.

because everybody is on the same network, all the computer are linked together, and a computer can read where from someone is connected. It would technically be possible for the MIT server to prevent access by French computers. The court can hold such an injunction. However, many Internet's sites[132] permits one to surf anonymously on the Web. By way of these servers, one can surf through every kind of site and their identity, and place of connection, is not revealed. The Internet also allows one to send E-mail to someone without its being able to be traced back.[133] In the case just explained, the MIT server could be sued by Mitterrand's family in front of an American court, which could apply the French law. But let's take another example. Salman Rushdie's books are forbidden in Iran. An American could scan one of his book and put it on the Internet, and therefore enable someone in Iran to read the book. The Government from Iran could sue the American server in front of an American court, but, the American court will not apply the Iran law forbidding Salman Rushdie's books.

The situation will be different if the two involved countries are democratic or develop political or friendship links. A good example is the "*Playmen*" [134] case held by the United States Supreme Court, South District of New York. An agreement was binding Playboy and Chuckleberry barring the latter from selling or distributing its "Playmen" magazine in the United States. The editor put the magazine on the Internet[135], it was therefore possible to view it within the United States. The court held that the Italian Internet site "permitting pictorial images to be downloaded to and stored upon computers of subscribers amounted

---

[132] E.g., http://www.anonymiser.com.

[133] E.g., http://www.srv.net/~allenh/jordan/anoy.html.

[134] Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032 (1996).

[135] http://www.playmen.it

to "distribution"[136], and then ordered the editor to "shut down the Playmen Lite service".[137] The court does not, however, bar Chuckleberry from maintaining its site in Italy. The editor followed this injunction and this site is no more accessible from the United States.

Other examples of problems of applicability of law may be found in the law of publicity. The Internet and the web are a very good way for a company to make publicity. However, publicity and telemarketing are regulated by both American and European law, and the reglementation is very specific concerning tobacco and alcohol. In the United-States, commercials for cigarettes are allowed except on TV-set and on the radio. However commercials for tobacco are allowed in Japan, and therefore a Japanese server could make this kind of publicity, which may be viewed in United States or Europe. It is even possible to buy every kind of cigarettes or cigars on the Internet, without any restriction of nationality or age.[138]

The law is unable to solve the problem of infringement in these type of cases and needs the help of the technology to close web sites to some computers. The law orders the technology to close one infringing Web sites. This brings up again the issue of free speech on the Internet, and the problems of legal regulation. Answers to these questions will be proposed in the second chapter.

Now that the relevant rules have been described and discussed, and the legal scope of the Internet defined, it is time to see how and against whom these rules will apply. It has been said that, because of the transnational nature of the Internet, it will be very difficult to enforce such laws. The only way to accomplish enforcement is to organize a system of penalties. For each infringement, liability has to be sought and the person responsible sued. How it is possible to establish liability on the Internet is the topic of the second section.

---

[136] 939 F. Supp. 1032.

[137] Id. at 1045.

[138] E.g., http://www.hollyent.com/adsmike/cigarett.htm
Http://www.cigarexpress.com.

SECOND PART: THE LIABILITY OF THE ACTORS OF THE INTERNET

Before using the Information Superhighway, the different actors of the Internet[139] must ask themselves certain questions related to their potential liability and rights in this new world. Is it possible to navigate or surf the Web with complete impunity? Is a provider liable for the wrongs of its users? What can an individual do if someone libels on him on the Internet or uses his copyrighted work without his authorization? These are a sample of questions that actors have to be aware of to enforce their rights in the network, and to undrstand how to establish liability and seek remedy, if their rights have been violated. They must also understand how and by whom their own liability can be engaged.

Liability may be criminal in cases of unauthorized hacking, defamation or child pornography; or it may be civil, as in cases of copyright infringement. Both criminal and civil liability may be engaged simultaneously.

Because of the nature of the Internet, it is often not easy to find the author of the damage in order to sue them and seek remedy. Consequently, providers, rather than authors, are sometimes held accountable for the liability.

The most common remedy ordered in case of liability, is in form of monetary damages. It is also possible to seek the cessation of the damage by, for example, withdrawing from the Web site the libelous information. The right of reply may also be very efficient because of its rapidity. It enables someone to answer a libel by the same mean the libel has been done.[140]

---

[139] This schema will explain briefly who are these actors:
Author ⇨ Server ⇨ Service provider ⇨ Telecom ⇨ User.

[140] It is often used in the press: A writes a libel in the newspaper on B. B reads it, he has the right to compel the newspaper to publish his answer to the libel.

No controversy surrounds the right of an injured party to seek damages from the tortfeasor. An individual user who commits torts, such as reading private E-mail or publishing defamatory or obscene messages, will surely be held liable. Controversy does however surrounds the issue of the extend to which the system operator (sysops) can also be held liable when a user commits such tort.

This section is going to explain how, and under what circunstances, it is possible to engage the liability of the different actors of the Internet. The liability of each actor will be studied individually.

I] Liability of the user[141]

The liability of the user may be sought by three actors: an author, the sevice provider, and another user[142].

A) Liability sought by the copyright owner

The author of a copyrighted work who navigates on the Internet and notices that his rights have been infringed upon may sue the infringer. The rights of the author on the Internet will be discussed in detail in the first part of the second chapter of this work.

In the United States, the Copyright Act of 1976 applies.[143] In France the Copyright Act of 1957 is the relevant rule.[144]

---

[141] The one who emits the information.

[142] The one who receives the information.

[143] Copyright Act, 17 USCA §§ 101 et seq.

[144] Loi No 57-235 du 11 mars 1957 amended by Loi 85-660 du 3 juillet 1985 relative aux droits d'auteur.

B) Liability sought by the service provider

The user may be liable towards the provider if he uses its service without the required authorization (for example, he did not pay for access priviledges, or the network is private), or because he causes damages on the network, for example by planting viruses or destroying data.

C) Liability sought by another user

There are many possibilities of conflict between users of the Internet. A user may fraudulently use someone else's password or credit card number to access private or paying sites,[145] may write defamatory or obscene messages, may violate privacy by entering private E-mail, may put viruses on the Web, or may infringe copyrights. The users are liable for any torts they commit on-line.

Liability for defamation and invasion of privacy are the most common and will be studied more extensively.

1) Liability for defamation

In the United States, the laws of liability for defamation are determined by each state. To sue someone for defamation, it is necessary to apply the tort law of that state. In such cases, the laws are the same on and off the Internet.

In France, the defamation is defined in the law of 1881[146]. The defamation involves a precise statement. The criminal liability, only of the author directly responsible for the

---

[145] Like pornographic or some games sites. See http//:www.secondworld.com.

[146] Loi du 29 juillet 1881, article 29.

defamatory message, may be engaged. (Article L 226-10 of the French Code Penal). Financial remedies may be sought by suing the author for his civil liability. The right to seek remedies is based on the article 1382 of the French Civil Code. This article states that anyone responsible for any statement which results in damages to an individual may be compelled to provide restitution to the injured party.[147]

In England, the first case of defamation on the Internet that resulted in establishment of liability of the author of the message was held in December 1993: Dr. Laurence Godfrey engaged liability and sought remedies against Dr. Philipp Hallam-Baker for "libel or alternatively slander in respect of articles posted on the Usenet computer network".[148]

2) Invasion of privacy

Account holders have the right to expect that their on-line affairs, such as personal or confidential business information, will remain private. However, because of the extraordinary power of the Internet, and because of the network itself, this expectation may not always be hold true. The magazine Fortune warns of how easily a company may be penetrated and its secrets stolen.

> "It was the week before Christmas, and the employees of XYZ Corp. were loging off a successful year with holiday parties at company headquarters in NY City. Meanwhile, inside their locked, darkened offices, not a creature was stirring, not even a computer mouse - or so they thought. Unbeknownst to the merrymakers, a team of professional hackers in Texas was preparing to invade XYZ's systems from 1,600 miles away." [149]

---

[147] Article 1382 du Code Civil: "Tout fait quelconque de l'Homme qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer."

[148] D. R. Johnson et al., *Computer Viruses: Legal and Policy Issues Facing Colleges and Universities*, 54 Educ. L. Rep. 761, 766 (1989).

[149] *Who's reading your e-mail,* FORTUNE, Feb. 3, 1997, at 57.

Fortune concludes:

> " Nutcrackers's success attests to what every technology manager knows: The more the computers of the business world become interconnected -via the Internet and private networks- the more exposed they are to break-ins." [150]

Users who intrude into the affairs or steal the identity of others are liable for invasion of privacy. In the US, First and Fourth amendments of the US Constitution[151], and the Electronic Communication Privacy Act (ECPA)[152] protect personal privacy against unlawful government intrusion.

The important provisions of the ECPA are outlined in the two chapters of Title 18 (Crimes and Criminal Procedures) of the United-States Code. The first chapter (119) is entitled "Wire and Electronic Communications Interceptions and Interceptions of Oral Communications". It focuses on the act of intercepting a private electronic communication.[153] Violation of these provisions of the ECPA can result in fines, and/or imprisonment for no more than five years[154]. Anyone who feels that their privacy has been violated in such a way can sue the responsible party for civil damages. The second chapter (121) is entitled " Stored Wire and Electronic Communications and Transactional records Access" [155]. This further

---

[150] Id. at 58.

[151] U.S. CONST. First and fourth Amendment.

[152] Electronic Communication Privacy Act of 1986, 18 U.S.C.§§ 2510 to 2711.

[153] As far as computer communications are concerned, any government agent, business, or individual who does or tries to do any of the following is acting in violation of the law:

- intentionally intercepts any electronic communication;
- intentionally uses or discloses the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of the ECPA.

See: 18 U.S.C. § 2511

[154] 18 U.S.C. § 2511(4)(a).

[155] Under this section, it is illegal intentionally to:

1- access without authorization a facility through which an electronic communication service is provided

2- exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

criminalizes hacking activity committed for purposes of commercial advantage, malicious destruction, damage, or private commercial gain. The punishment includes a fine of not more than $250,000 and/or imprisonment for no more than one year. Other cases of hacking for purposes other than those listed above can be punished by a fine of no more than $5,000 and/or imprisonment for no more than six months.[156]

The right of privacy is also protected by the common law of privacy, which permits a tort action for damages resulting from unlawful invasion by another user.[157] This tort has been applied in cases of telephonic surveillance.[158] Invasion of privacy may also be sentenced by the criminal liability of the wrongdoer.

In Europe, privacy is protected by Article 8 of the European Convention for Human Rights, which insures for everyone respect of privacy and of secret correspondence.

In France, several laws exist to protect the right to privacy. Article 9 of the civil code[159] and L 226-1 of the criminal code, which sanctioned by 1 year of imprisonment and a penalty of 300 000 FF ($ 60.000) anyone who violates by any way someone's privacy.[160] The Computer Fraud Act of 1988[161] outlaws all nonauthorized intrusion in any computer system by any means. Privacy is also protected by the "treaty of the Internet". This treaty is comparable to a "good behavior code" or also called "Netiquette". It details the protection of privacy in its article VII B (2) and (3). It states that the correspondence must remain secret

---

See: 18 U.S.C § 2701(A).

[156] 18 U.S.C. § 2701(b).

[157] See Restatement (Second) of Torts s 652B (1977): "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."

[158] Billings v. Atkinson, 489 S.W. 2d 858 (1973).

[159] Loi du 17 juillet 1970.

[160] New Criminal code, Art L226-1.

[161] Loi No 88-19 du 5 janvier 1988 relative à la fraude informatique.

even from employers, and that users may navigate anonymously on the Internet. Presently, this "treaty" is only a proposition

With these laws, protection against defamation and against privacy are possible on the Internet. Rules exist and users will apply these rules to enforce their rights in the cyberworld. Nevertheless, two problems arise with the application of these principles. The first problem that arises with enforcement of privacy laws, is reconciling a suit with the constitutional right of freedom of speech.[162] The second is finding the user who wrote the defamatory message or intruded on another privacy.

It is not simple to find the individual who causes the damage because of the increasing numbers of users who navigate anonymously[163] on the Internet, and who send anonymous mail through the Internet the E-mail.[164] More over, a large percentage of the activities that take place on the Web occur between people using assumed names (handles) or pseudonyms. This is the main reason why plaintiffs will try to establish the liability of actors other than the authors of the libel. The question that arises, is whether the providers should be held liable.

II] Liability of the providers

There are three basic providers on the information superhighway. The first one is the content provider, which communicates information in any form via electronic media.

---

[162] See infra Chapter II, First part.

[163] Anonymous remailers make messages sent on computer networks virtually untraceable. An anonymous remailer is a computer configured to receive an incoming message, automatically strip it of any trace to the sender's identity, and then forward it to its addressee.
E.g., remailer@flame.alias.net

[164] E.g., for anonymous surfing: http://www.anonymizer.com

Newspapers that are published on the Internet are traditional content providers.[165] The fact that the information is being transmitted via electronic impulses rather than ink on newsprint does not affect the writer's and publisher's status as publishers[166]. The second provider may be called the "pure access provider." It furnishes the electronic connection for two or more content providers to communicate. For example, MCI provides MCI Mail, an electronic communications system by which subscribers connect electronically, much as telephone subscribers communicate through the telephone company. MCI does not communicate itself, but provides the means by which others may communicate.[167] The third provider is both an access provider and a service provider. It provides a direct connection and a common forum, such as a BBS (Bulletin Board System) for public communication among subscribers. The proprietor and operator of a BBS (called an Internet Service Providers [ISP], or system operator [sysop]) may be a commercial operator such as CompuServe, Prodigy, or America Online.

ISPs are potentially liable for the on-line torts committed by their customers within their own system, or for torts committed on the Internet through the access they provide. This liability may be sought by an individual user or by an infringed copyright owner. The problem remains, however, of how this responsability can be legally established.

A) Liability sought by the user

As described in the previous part, the user may engage the liability of the ISP for defamatory messages. The user may also engage liability for invasion of privacy.

---

[165] E.g., http://www.nytimes.com is the web site for the New-York Times.
http://www.lemonde.com is the web site for Le Monde.

[166] See Daniel v. Dow Jones & Co., 520 N.Y.S.2d 334 (1987).

[167] Eric Schlachter, *Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions*, 16 Hastings Comm & Ent. L. J 87, 90 (1993).

1) <u>For defamatory or obscene messages</u>

To understand how to address the problem of defamation in the cyberworld it is helpful to view this defamation in the context of the familiar principle in libel law, known as the 'graffiti principle'.

In 1952, an appellate court[168] found a tavern owner liable for a defamatory message scrawled on the bathroom of his tavern. The court deemed the owner guilty of republication of the libel, stating: "republication occurs when the proprietor has knowledge of the defamatory matter and allows it to remain after a reasonable opportunity to remove it." [169] In a separate case, the court limited the republication liability, adding the requirement that, for imposition of liability to be legitimate, the defendant must have somehow invited the public to read the allegedly libelous statement,[170] thereby committing a fault.[171]

In the domain of the press, three categories of people potentially responsible for defamation may be distinguished. First, publishers of magazines and newspapers may be held liable for a defamatory statement, because they are in complete control of the writing, editing, and publication of the material they publish[172]. Second, distributors,[173] such as libraries or bookstores, may be held liable, but only if they know or have reasons to know about the defamatory statement.[174] Third, common carriers, operators who provide a specific

---

[168] Hellar v. Bianco, 244 P.2d. 757 (Cal. Dist. Ct. App. 1952). The message stated in essence "call this number for a good time and ask for Isabelle". Isabelle's husband call the tavern and asks its owner to remove the message. It did not do it.

[169] Id. at 759.

[170] Scoot v. Hull, 259 N. E. 2d 160 (Ohio Ct. App. 1970).

[171] See New York Times Co. v. Sullivan, 376 U.S . 254 (1964).

[172] E.g., Gertz v. Robert Welch, Inc., 418 U.S. 323, 346 (1974).

[173] Also called sometimes "secondary publishers".

[174] E.g., Lerman v. Flynt Distrib. Co., 745 F.2d 123 (2d Cir. 1984) (magazine distributor), cert. Denied, 471 U.S. 1054 (1985).

service to whomever desires it, allow subscribers to transmit information of their choice without control. Even if the common carrier is aware that a defamatory statement exists, he is generally not held liable for its users' defamatory statement.[175]

The required elements for a claim of defamation are specifically outlined in the Restatement (Second) of Torts. They are (1) a false and defamatory statement concerning another, (2) an unprivileged publication to a third party, (3) a fault amounting at least to negligence on the part of the publisher[176], and (4) either special harm or actionable conduct irrespective of special harm.

The way defamation is dealt with outside the Internet where the author of the message is unknown, but its carrier is known, is well defined. Some courts have, however, already had to face the novel problem of defamation on the Internet. If the same principles were applied to the Internet as have been described for the press, an ISP could be found libel if it was aware of an allegedly libelous posting and undertook to nevertheless ratify the communication.

Prosser has noted, that "the question is to what extent should one who is in the business of making available to the general population what another writes or says be subject to liability for the defamatory matter that was published."[177]

Two important cases deal with individual Internet users seeking remedies against their ISPs for defamatory messages. The Courts have made an analogy between ISP liability and newspapers or bookstores' liability. The issue remains however whether ISPs can be held liable for defamatory statements uploaded by their customers, and then whether these ISPs function as primary publishers, distributors, or common carriers as defined in Title II of the Federal Communication Act of 1934. After a quick explanation of the facts surrounding

---

[175] E.g., Anderson v. New York Tel. Co., 320 N.E.2d 647, 649 (N.Y. 1974).

[176] Maliciously is required if the victim is a public figure.

[177] W. Page Keeton et al., *Prosser and Keaton on the law of torts §111*, at 803 (5th ed. 1984).

these cases and of the decisions held by the court, we will see how it is possible to apply these decisions to determine the extent of liability of an ISP.

The first case, *Cubby, Inc. v. CompuServe Inc* was decided by the Southern District of New-York in 1991.[178] CompuServe is one of the largest of the commercial on-line services. It is a general information service, or "electronic library" that permits access to thousands of information sources. Camron Communications, Inc. (CCI) contracted with CompuServe to manage and control the Journalism Forum. CCI had editorial control over the forum. Rumorville USA is a publication available on the Journalism Forum that provides information about broadcast journalism and journalists. CompuServe has no power to review the contents of Rumorville prior to it being uploaded. In 1990, Cubby Inc. developed a computer database to compete with Rumorville. The source of the dispute was allegations that Rumorville published false defamatory statements about Cubby and its developer Robert Blanchard. Cubby and Blanchard sued for libel. CompuServe argued that it acted as distributor rather than as publisher of this alledged defamatory statements, and that it did not know, and had no reason to know, about the statements. CompuServe therefore argued that it could not be held liable for the statement's content. CompuServe based also its arguments on the fact that CCI has contracted to "manage, review, create, delete, edit and otherwise control the contents"[179] of the Journalism Forum.

The court stated that " CompuServe has no more editorial control over . . . publication than does a public library, bookstore, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so."[180] The court, comparing CompuServe to a distributor added "First Amendment guarantees have long been recognized as protecting

---

[178] Cubby Inc. v. CompuServe Inc. , 776 F. Supp. 135 (S.D.N.Y. 1991).

[179] Id. at 137.

[180] Id. at 140.

distributors of publications . . . Obviously, the national distributor of hundreds of periodicals has no duty to monitor each issue of every periodical it distributes. Such a rule would be an impermissible burden on the First Amendment."[181] The court found CompuServe to be a distributor only and therefore not liable.

The second case *Stratton Oakmont, Inc. V. Prodigy Servs. Co.*[182] was tried by the Supreme Court of New-York in 1995.

Prodigy is a computer on-line service with at least 2 million subscribers. Prodigy, as a part of its services, contracts with Bulletin Board Leaders, who, among other things, participate in board discussions. "Money Talk" is one of Prodigy's bulletin boards, where members can post statements regarding stocks, investments and other financial matters. In October 1994, an unidentified person posted on Money Talk allegedly defamatory statements about the plaintiff, Stratton Oakmont Inc., a securities investment banking firm. Stratton sued Prodigy and the unidentified person who had posted the statement on Money Talk for per se libel. The plaintiff argued that Prodigy was a publisher because of its family oriented service policy, and that it was therefore liable for any defamatory statements posted on its bulletin board. Strattons arguments were supported by the existence of a software screening program with an emergency delete function, which could be used by Prodigy's Bulletin Board Leaders. The issue for the court was whether or not Prodigy exercises enough editorial control over bulletin board content to be considered a publisher, whit the same liabilities as a newspaper publisher.

The court distinguished this case from *Cubby* on two grounds: first, Prodigy maintained to the public and to its members that it is in control of the content of its computer bulletin boards, and second, Prodigy implemented this control through its automatic software screening program, the guidelines of which Board Leaders are required to enforce. The court

---

[181] Id. (quoting Lerman v. Flynt Distrib. Co., 745 F.2d 123, 139 (2d. Cir. 1984), cert. Denied, 471 U.S. 1054 (1985)).

[182] 23 Media L. Rep 1794 (1995).

held therefore that Prodigy had an editorial control over its bulletin board, making it a publisher rather than a distributor, and that Prodigy is therefore liable for the contents of its bulletino board.

The liability of an ISP will be different whether it acts as and is then considered as a distributor, a publisher, or a common carrier.

→ ISP as a distributor

The ISP is considered a distributor if it has no more editorial control over publication than does a public library. The distributor does not know and has no reason to know of the allegedly defamatory statement. In such a case, the ISP cannot be held liable for any defamatory or obscene message sent through its service.

→ ISP as a publisher

The ISP is considered a publisher if he it controls the content of the messages posted on its service and therefore has the possibility to be aware of the defamatory or obscene statement. In this situation it can be held liable regardless of its fault in publishing the material. The standard of liability is negligence[183] rather than strict liability.

→ ISP as a common carrier

Common carriers are defined in Title II of the Federal Communications Act of 1934[184]. If placed in this category, commercial on-line services would not be liable for defamatory statements transmitted by users.[185] However few on-line services will agree to be classified as common carriers since they are closely regulated by the federal government and subject to intense scrutiny.

---

[183] For non-public figures.

[184] "Common carrier means any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this chapter; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier".
47 U.S.C.A. s 153(h).

[185] Restatement (Second) of Torts s 581 cmt. b.

In the view of this regime of liability, it is likely that commercial on-line services will face difficult choices in what roles they will play in influencing the content they carry. A service might choose to institute very strict standards to prevent any defamatory or obscene messages from reaching its bulletin boards. Implentation of strict control would lead the ISP to delete some content and that would run counter to the freedom of speech. Alternatively, it might choose to take a totally hands-off approach in order that it appear to have no editorial control, so as to fall under the auspices of a distributor rather than a publisher.

An addition consequence of the liability of the ISP will be an increase in the cost of the monthly and hourly fees paid to ISP. If ISP are to be held liable, they will certainly insure the risk of liability.

One alternative way to solve the problem of defamatory messages is by the automatic right of reply. This alternative would allow aggrieved users to vindicate themselves through the same medium in which they were allegedly wronged.

2) For intrusion of privacy[186]

An ISP may face liability if it negligently enables someone to intrude wrongfully in the private affairs of another user of th system. The ISP has the possibility to ensure the security of its system, which contains confidential information: passwords-screening programs, cryptography etc. Therefore, the ISP may be held liable for failing to protect customers or for otherwise not undertaking his affirmative duty to take action to protect customers' privacy. The most recent statutes[187], however include some protections for ISPs against charges of inadequate privacy protection. Congress recognizes that overuse of vicarious liability will deter useful Internet growth.

---

[186] See supra, page 41, for more developments.

[187] The Communication Decency Act of 1996 (47 USCA ss 223) and the Electronic Communications Privacy Act of 1984 (18 USCA ss 2511).

B) Liability sought by a copyright owner

For the same reasons as above[188], an author whose copyright has been infringed by an user will often prefer to seek remedies against the ISP than against the author of the infringement. How the liability of an ISP may be sought for copyright infringement of an user is the subject of this paragraph. To understand this regime of liability of an ISP, it is useful to know how the Internet may permit a user to infringe protected copyright, what is the copyright law, and what is the policy in regards to copyright infringement outside cyberspace. An analysis of these issues will permit the drawing of a liability regime of an ISP in cases of copyright infringement.

A last paragraph will deal with the propostion of ISP liability introduced in the Congress by the Working Group on Intellectual Property Rights of the Clinton Administration's National Information Infrastructure Task Force (White Paper).[189]

1) How the Internet permits users to infringe copyrights?

Digital audio allows infinite duplication of perfect copies of music which equal the original and which are themselves easy to duplicate and distribute by the way of computers. The user has just to request a specific song on a web site[190] and the song is transmitted in digital form through the network, where upon the user has only to record the song onto a compact disc.[191] The process is the same for movies. For example, Time Warner, Inc., plans to activate its computerized fiber optic network to deliver movies on demand in Orlando,

---

[188] Anonymous user, and user who have pseudonyms.

[189] See Chapter I, First part.

[190] E.g., http://www.audionet.com/music.

[191] See N. Jansen Calamita, *Coming to Terms with the Celestial Jukebox: Keeping the Sound Recording Copyright Viable in the Digital Age*, 74 B.U. L. Rev. 505, 519.

Florida, in the near future.[192] The system includes storage of vast digital libraries of entertainment and information which could potentially be reproduced without authorization on computer networks.[193] Copyrights on photographs may also be infringed, photos may be digitized using scanners Stock photo agencies now store photographs on computer disks in digital form. Filmless electronic cameras are being developed to record photographs on video floppy disks. Photographs, once in digital form, can easily be edited, manipulated, or transmitted via the Internet. Finally, new photocopying technology, when coupled with a digital scanner and character-recognition software, allow entire books to be converted into digital form with ease. When the infringer scans the book and downloads it on the Internet, any user has just to print the book to read it.

2) What is the copyright law

Congress enacted the Copyright Act in 1976.[194] Section 106 of the Act grants the owner of a copyright the exclusive right to reproduce the copyrighted work, prepare derivative works based on it, distribute copies, and, in certain instances, to publicly perform or display the work.[195] To establish a claim of copyright infringement, the copyright holder must demonstrate (1) ownership of a valid copyright and (2) unauthorized exercise by the defendant of one of its exclusive rights.[196] There are three types of infringement: First, direct infringement, established by the plaintiff when he proves his ownership of the protected work

---

[192] See Joia Shillingford, *Survey of International Telecommunications*, Fin. Times, Oct. 3, 1995, at XXV.

[193] See http://pathfinder.com/ew/movies.

[194] 17 U.S.C.A. s 102(a) (1976).

[195] Id. s 106.

[196] See e.g., Baxter v. MCA, Inc., 812 F.2d 421, cert. denied, 484 U.S. 954 (1987).

and actual copying by the defendant; second, contributory infringement[197], where there is direct infringement by a third person and the defendant "with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct"[198]; and third, vicarious liability, where the plaintiff has to show that the defendant not only had the right or ability to supervise or control the actions of the infringer, but also had a financial interest in "the exploitation of the copyrighted material"[199], that he received a direct financial benefit from the infringement. In such a case, there must be a corresponding direct infringement by a thrid person.

An examination on how these theories have been applied outside the cyberworld in cases analogous to the copyright problem presented by ISP is helpful to define the ISP's liability regime.

3) Liability for copyright infringement outside the cyberworld

The Copyright Act defines three grounds against copyright infringement: direct infringement, contributory infringement, and vicarious liability.

Direct infringement is the most straigforward and does not require discussion. An example of contributory infringement however may be helpful to elucidate this more complicated form of liability.

A defendant may be held liable for contributory infringement in two cases: if he acts in concert with the direct infringer by contributing labor to the infringing activity, or if he acts in concert with the direct infringer by providing materials or equipment necessary for the infringement to occur. Contributory infringement is distinguishable from vicarious

---

[197] Courts have created the doctrine of contributory copyright infringement by analogy to patent law: See Harper v. Shoppel, 28 F. 613 (C.C.S.D.N.Y. 1886).

[198] Gershwin Publishing Corp. v. Columbia Artists Management, Inc, 443 F.2d 1159, 1162 (1971).

[199] Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (1963).

liability because it requires knowledge of infringing activity and some sort of cooperation between the defendant and the direct infringer.

A manager of concert artists and a creator and producer of local concert associations were held liable for contributory infringement because they knew that their artists included copyrighted compositions in their performances and had not secured copyright licenses.[200]

Two sets of decisions have been made concerning vicarious liability. The first set of cases (dance hall cases) hold that a dance hall proprietor is liable for copyright infringement resulting from the performance of a musical composition by a band or orchestra. The proprietor is liable when he could control the premises, and obtained a direct financial profit from the audience, who paid to enjoy the infringing performance.[201]

In the second set of cases (landlord-tenant cases), the defendants rented out booth space for an event at which some of the booth renters committed copyright infringement, by selling protected work. The court decided that, if the landlord has no knowledge of the infringement of its tenant, and if he exercises no control over the leased premises, he will not be held liable.[202]

According to the decision of the court in these cases, two factors are relevant to determine the liability of the defendant: supervision/control and financial benefit. These factors imposed liability even though the defendant was unaware of the infringement.[203] We will now focus on infringement cases in the domain of Internet.

---

[200] Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159 (1971).

[201] Buck v. Jewell-Lasalle Realty Co., 283 U.S. 191, 198-199 (1931).

[202] See e.g., Deutsch v. Arnold, 98 F.2d 686 (1938).

[203] See Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304 (1963).

4) Cases dealing with copyright infringement on the Internet

Two important cases have dealt with ISP liability in copyright infringement.[204] *Playboy Enterprises, Inc. v Frena* [205] concerns photograph copyright infringement. Playboy filed suit against Frena, the operator of Techs Warehouse Bulletin Board Service, alleging that it infringed Playboy's copyright by distributing copies of Playboy's protected photographs. Frena admitted that the images were available on its system, and that the photographs had been downloaded by its subscribers. But Frena did not know that the photographs had been uploaded by subscribers onto bulletin board. However it claimed that the images were uploaded by subscribers over whom Frena had no control, making this innocent infringement by Frena. Moreover, Frena contented that the affirmative defense of fair use precluded a finding of infringement. The court noted that even innocent infringers are liable[206] and that neither de minimis non curat lex, nor fair use justified Frena's infringement[207]. Therefore, the court held Frena (the ISP) liable for violating the plaintiff's exclusive right to publicly distribute and display copies of its work[208], making this a case of direct infringement.

The second case, *Sega Enterprises Ltd. v. Maphia*, [209] followed *Playboy* and concerned copyrights of Sega video games. The defendant, Maphia, is a bulletin board operator open to the public. Most of its users communicated using pseudonyms. The

---

[204] See also for a similar decision: Frank MusicCorp. v. Compuserve, No. 93 Civ. 8153 (S.D.N.Y. filed Nov. 19, 1993).

[205] Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (1993).

[206] Judge Schlesinger noted that "intent to infringe is not needed to find copyright infringement" Playboy Enterprises, 839 F. Supp. at 1559.

[207] Id.

[208] Id. at 1556-57.

[209] Sega Enterprises Ltd. v. Maphia, 857 F.Supp. 679 (1994).

defendant intentionally placed copyrighted materials on the bulletin board service it operated. The court held that Sega had established a prima facie case of direct infringement by showing that unauthorized copies of games were made when the games were uploaded on the bulletin board with the knowledge of the defendant, and that therefore Maphia's "role in the copying, including provision of facilities, direction, knowledge, and encouragement amounts to contributory infringement",[210] even though Maphia did not know exactly when files were uploaded or downloaded. Judge Wilken noted that defendant was unlikely to establish fair use.[211]

These two decisions were the basis for an important subsequent decision like *Religious Technology Center v. Netcom*[212]. In this case, a critic posted an allegedly infringing excerpt by way of a bulletin board service which has access to the Internet via Netcom. Netcom argued that it had no control over subscribers' postings, and that its knowledge of the infringement was "insubstantial". It did not sufficiently participate in the writer's alleged direct infringement to be liable as a contributory infringer.[213] The court found that Netcom was not directly liable for copies that were made and stored on its computer,[214] and that it did not receive direct financial benefit from infringing activity necessary to hold it vicariously liable.[215] The court faced the problem of knowledge to decide whether Netcom could be held liable for contributory infringement. It noticed that Netcom was given notice of an infringement claim, asking him to remove the infringing materials, before the critic has

---

[210] Id. at 686.

[211] "Even if defendants do not know exactly when games will be uploaded to or downloaded from the Maphia bulletin board, their role in the copying, including provision of facilities, direction, knowledge and encouragement, amounts to contributory infringement".
Id. at 686-687.

[212] 907 F. Supp. 1361 (1995).

[213] Id. at 1373.

[214] Id.

[215] Id. at 1377.

completed his infringing activity. Netcom did not look at the postings, and admits that if it had done so, it would have "triggered an investigation into whether there was infringement or not."[216] Then, because Netcom received a letter from the plaintiff, he is sensed to have knowledge of the infringement. Therefore, the court found Netcom liable as a contributory infringer because it permitted user infringement. This was deemed a sufficient participation for liability.[217]

The study of these three cases leads to a problem of interpretation and application of the Copyright Act. The United-States District Court of Florida, in *Playboy*[218] held the ISP liable for direct infringement. In *Sega*[219], the United-States District Court of California cited the previous case as finding a contributory infringement, and the same court in *Netcom*[220] made the same ruling and denied any direct infringement by Netcom[221]. These decisions, though somewhat contracdictory and controversial, are nevertheless helpful in defining the liability of ISPs in cases of copyright infringement by users.

5) Application to draw the liability of ISP for user's copyright infringement

In the context of ISP liability, courts must carefully distinguish between direct and contributory copyright infringement, and vicarious liability.

---

[216] Id. at 1374.

[217] Id. at 1382.

[218] Supra note 205.

[219] Supra note 209.

[220] Supra note 212.

[221] 970 F. Supp. at 1372
"Where the infringing subscriber is clearly directly liable [for these acts], it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringing is nothing more than setting up and operating a system that is necessary for the functioning of the Internet."

→ May the ISP be liable for direct copyright infringement?

If the copyright holder can prove that the ISP infringed his rights by distributing and displaying copies of his work through the Internet, the ISP may be held liable, regardless of whether or not the ISP was aware of the copyright infringement.[222]

→ May the ISP be liable for contributory infringement?

Liability for contributory infringement demands a knowledge and a substantial participation factor. The relevant time frame for knowledge of the infringement is when the ISP provides its services to allow the infringer to infringe plaintiff's copyright (actual knowledge). If the plaintiff can prove the knowledge element that the ISP was aware of the infringement or had reasons to know it[223], the ISP will be liable for contributory infringement since it failed to cancel the infringing message. However, the knowledge must be reasonable. If the ISP did not have the opportunity to verify the claim for infringement (because of fair use defense for example), its lack of knowledge is reasonable and he cannot be held liable for its user's infringement.

If the ISP allows the infringer, once accused, to stay on its service and does not take any measures to prevent further damages, the substantial participation factor is fulfilled.

Therefore, an author whose copyrighted works are infringed may seek remedies against the ISP by seeking its liability for contributory infringement.

→ May the ISP be liable for vicarious liability?

The plaintiff has to show that the ISP has the right and ability to supervise and control the conduct of its subscribers. A burden of proof may lead to the fulfilment of this requirement (however, one of these elements in itself is not enough): terms and conditions of the contract between the ISP and the user (infringer) specify that the ISP reserves the right

---

[222] See Playboy, 839 F. Supp. 1552, 1559: "There is irrefutable evidence of direct copyright infringement in this case".

[223] For example in Sega, even in Maphia did not have actual knowledge of the infringement, the court inferred that it had reason to know that direct infringement was occurring since Maphia sold copying devices and discussed downloading games on the service. 857 F. Supp. at 681.

to take remedial action against the subscriber with an easy software modification; the ISP may identify postings that contain particular words[224] or come from particular individuals; and the ISP can delete specific postings.

Then, the plaintiff must also prove that the ISP earned a direct financial benefit from the infringement. This will usually be difficult to prove because ISPs receive fixed fees that do not increase because the ISP has permitted the infringement, and the infringement does not enhance the value of the ISP's services to subscribers and does not attract new subscribers. There would, for example, be a direct benefit of the infringement if the ISP accepts from the infringer an amount of money to post the infringing message on its service.

For these reasons, claims of vicarious liability will often fail and will not help the plaintiff in seeking the ISP's liability.[225]

If liability is recognized by the court, it may order the ISP to stop its service providing the infringing material, with a penalty, and to pay damages[226] to the copyright holder.To avoid its liability for copyright infringement, the ISP may raise the defense of fair use[227]. If the four factors set out by the Congress are fulfilled there will be no infringement and

---

[224] See for an example of control (attention, it is not a case of copyright infringement, but a case of ISP liability for defamatory messages): Stratton Oakmont, Inc. v. Prodigy Service Company, 63 USLW 2765 (1995).

"Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards" and "Prodigy implemented this control through its automatic software screening program, and the guidelines which Board Leaders are required to enforce."

[225] However, the plaintiff can try and combine claim for vicarious liability with claim for direct and contributory infringement.

[226] Copyright remedies are the following:

- Injunctive relief is authorized by the Copyright Act. 17 U.S.C. § 502.
- Actual damages are available under the Copyright Act including lost profits and profits gained by the infringer to the extent not counted in the copyright owner's lost profits. 17 U.S.C.§ 504(b).
- Alternatively, statutorydamages of up to $20,000, or up to $100,00 if the infringement is wilful, are available. 17 U.S.C.§ 504(c).

Attorney's fees are available if the work had a registered copyright before the act of infringement. 17 U.S.C. § 505.

[227] 17 U.S.C. §107.

therefore no liability.[228] Sometimes, the parties may settle an agreement, instead of seeking a court injunction. In *Frank Music Corp. v. CompuServe, Inc.*,[229] Frank claimed that CompuServe was responsible for infringing copyrights in over 900 songs because it allowed its subscribers to upload and download digital sound recordings of the songs to and from CompuServe databases. The parties announced a settlement under which CompuServe agreed to obtain and pay for licenses from the licensing agency.

6) The Working Group proposal and the reactions

The White Paper supports strict liability for on-line service providers. It finds that ISP are in a "better position to prevent or stop infringement than the copyright owner. Between these two relatively innocent parties, the best policy is to hold the service provider liable."[230] According to the Working Group, "exempting or reducing the liability of service providers prematuraly would choke development of marketplace tools that could be used to lessen their risks of liability and the risk to the copyright owners", and would then "encourage intentional and willful ignorance"[231] on the part of the ISP.

This draft enables content owners to request that ISP immediately remove or prevent access to infringing woks. ISP could avoid all liability for copyright infringement if they favorably respond to the request. Copyright owners could also forego the fast track option

---

[228] 17 USC §107.

* The purpose and character of the work (criticism, use of commercial nature, or for non profit organization),
* The nature of the copyrighted work
* The amount and substantiality of the portion used in relation to the copyrighted work as a whole
* The effect of the use upon the potential market for or value of the copyrighted work.

[229] No. 93 Civ. 8153 (S.D.N.Y. Nov. 29, 1993).

[230] See Intellectual Property and the National Information Infrastructure: The Report on the Working Group on Intellectual Porperty Rights (1995) (the "White Paper"), at 117.

[231] Id. at 122-23.

and pusue litigation for copyright infringement. Finally, increased penalties would be imposed on those who "shocase" or encourage viewing of infringing works, and dimished liability will be granted for ISP who respond quickly to charges of infringement.

The White Paper has drawn a lot of criticism from the online industry.[232] Indeed, ISP have no way of policing what is transmitted on their network. The volume of material on a ISP system is too large to monitor or screen. More over they should not review the content sent on their network, because if they do so it is interfering in the right of free speech that every user owns. Exposure to strong liability of ISP would drive them out of business, causing the cyberspace to fail.

It is possible to seek the liability of the ISP, as a company. What about the liability of their directors? Their liability may also be engaged as manager of the company. Such a decision will soon be discussed by a German court. Bavarian state authorities charge the managing director of the German division of CompuServe with providing access to pornographic and racist material on the Internet. The Bavarian state prosecutor office says that the managing director has violate laws on youth protection and racism. He is accused of allowing the distribution of banned material even though he had "technical and organisational measures" available to prevent this. The authorities claim that CompuServe is infringing the law by providing access to computer games which celebrate violence and, in one case, include pictures of Adolf Hitler and swastikas, images which are banned under German law.[233]

---

[232] William W. Burrington, Assistant General Counsel for America Online, Inc., suggested that the following principles be included in any legislation:

- mandatory notification of infringement by content owners when they became aware of infringement coupled with an obligation on the part of providers to remove infringing material within a specified time;
- no obligation for providers to police transmissions; and
- no liability for infringement in cases where providers serve as mere conduits without generating or altering content (such as providing trunk line, processing, intermediate storage, and access software services).

[233] In 1995, CompuServe was already compel to close newsgroup known for their pornographic and racist content.

This first part permits the Internet actor to know the rules of the cyberworld. He knows under wich law he is going to navigate on the information superhighways and in front of which court he could be sued if he causes damages. He is also aware of how liabilities may be engaged, how it is possible to engage one's responsability and seek remedies, but also how his own liability may be sought.

Thanks to all this knowledge, he knows the rule of the game and can enter this new world in order to begin to surf the Internet. However, before becoming a real actor of the Internet, he needs to know more rules on its utilization. The knowledge of these rules is mandatory so as not to see his liability sought for a misuse of the huge oportunities offered by the cyberspace. The purpose of the following chapter will then to study how to use legally the Internet.

CHAPTER II

LEGAL USE OF THE INTERNET

A new user of the Internet who really wants to become a versatile actor in cyberspace has to know how to use it. The purpose of this chapter is not to provide technical explanations on how to plug one's computer to cyberspace and establish links to the network, but rather to study the policy of the network and how to use it legally.

Two main principles of law govern the Internet and regulate actors' behaviors in cyberspace. First, is the right of the author (copyright law), and second is the right of Free Speech.

FIRST PART: COPYRIGHT ISSUES

A great many works are distributed every day through the Internet. Legislation regulating copyright of these works is of concern to many players on the Internet. The owner of the intellectual property rights of these works, most often the publisher, has a huge interest in knowing what his rights are when his work is downloaded or distributed on the Internet. He has to know what kind of utilization of his work he can bar and what he can demand. The service provider has to know under what conditions it may put the author's work on its own site. If the work is utilized illegally, if the service provider infringes copyright, the author could be entitled to thousand of dollars in remedies, even if the service provider did not

know that it was infringing copyright.[234] The user will also wish to know which works on the Internet he is allowed to use without the author's authorization.

Besides, the importance of addressing copyright issues involving the actors of the Internet, it is also interesting to examine copyright law itself in the context of the Internet, since the purpose of copyright law the purpose of the Internet conflict. The Internet's purpose, dating from its creation in the 1960's, is the free flow of ideas, and the purposeful creation of a shared knowledge and information.

The aim of this section is, first, to give the author a clear view of what kind of control he can expect to have over his work once on the Internet (author's rights), and second, to make each actor of the Internet aware of the legal way in which to use the work without infringing the author's copyright, so as to avoid liability (user's rights).

I) What rights can the author expect to have over his work once put on the Internet?

We will see that, when an author puts his work on the Internet, he can expect it to be protected by the Copyright Act, and this protection grants him some rights over his work.

A) Can the author expects protection by the Copyright Act for his work on the Net?

To answer this question, it is first necessary to see what the general conditions are for a work to be protected on the Internet. Then it will be possible to determine what kind of work is protected.

---

[234] See Chapter I, Second part.

1) Is a work put on the Internet copyrightable?

To be protected by the copyright law, a work needs to fulfill the conditions required by the Copyright Act[235]. Paragraph 102 states that "copyright protection subsists (...) in original works of authorship, fixed in any tangible medium of expression, now known, or later developed."[236] To be protected, a work needs to be "original" and "fixed."

a) Originality

This term is not defined by the Copyright Act. It has therefore been the role of the courts to define the term. They have defined the word "original" to mean only that the work owes its origin to the author, that the work is independently created, rather than copied from other work.[237]

To constitute a "work of authorship", the work must pass a creativity "threshold", it must embody "some modest amount of intellectual labor".[238] The level of creativity necessary and sufficient for copyrightability has been described as "very slight", "minimal", and "modest".[239]

U.S. copyright protection extends only to expression. Ideas, procedures, processes, and systems are not copyrightable.[240]

---

[235] 17 U.S.C. §§ 101.

[236] 17 U.S.C. § 102.

[237] See e.g., Atari Games Corp. v. Oman, 888 F.2d 878 (1989).

[238] See e.g., Baltimore Orioles, Inc, v. Major League Baseball Players Ass'n 805 F.2d. 663, 668 (1986).

[239] See e.g., West Publishing Co. v. Mead Data Central, 799 F.2d. 1219, 1223 (1986).

[240] 17 U.S.C. 102 (b).
The United States Supreme Court stressed in 1990: "The most fundamental axiom of copyright law is that 'no author may copyright his ideas or the facts he narrates.' . . . Copyright assures authors the right to

For these reasons, the condition of originality is easily fulfilled in the cyberworld. As far as the criteria of originality is concerned, an author may create an original creative work that is copyrightable putting pen to paper, brush to canvas, or fingers to a computer keyboard.

b) Fixation

To be copyrightable, the works have to be "fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device:" [241] A work is fixed when "its embodiment in a copy or phonorecord . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration. A work consisting of sounds, images, or both, that are being transmitted, is 'fixed' (...) if a fixation of the work is being made simultaneously with its transmission." [242]

The condition "of more than transitory duration" is problematic for electronic documents created at the time of their communication on the Internet.[243] A representation of a program in random access memory[244] (RAM) is made with the understanding that the representation could be eradicated within milliseconds. Representations in RAM are typically made as part of a high-speed computational process, not for the purpose of permanent or stable storage.

---

their original expression, but encourages others to build freely upon the ideas and information conveyed by a work."
Feist Publications, Inc. v. Rural Telephone Service Company., 449 U.S. 340 (1990).

[241] 17 U.S.C. § 102.

[242] 17 U.S.C. § 101.

[243] E.g., the e-mail.

[244] It represents that part of a computer's memory in which data and computer program can be recorded temporarily. When a computer is turned off, the information stored in RAM is lost.

If the fact of putting an original work on the Internet is considered as fixing the work, the work will be protected. The fact of downloading the work (just to view it) is also a fixation, therefore downloading a protected work constitutes copying the work, which infringes the exclusive right that the author has to reproduce and make copies of the work.[245]

Two points of view may conflict at this time, between those who think that the condition for fixation is not fulfilled unless the work is saved to diskette, or hard drive[246] and those who think that every kind of communication, even by way of computer, is protected.[247] As it will be explained, copyright protection for works that appear on the Internet must be considered according to the category into which they fall. These categories of copyrightable works may very well determine the scope of protection and the exceptions to protection that pertain to a given work appearing on the Internet. Whether the work is fixed or not depends, in fact, on the nature of the work.

It must, however, be pointed out that the National Information Infrastructure Task Force declared in its White Paper that a copy is made when a work is placed into a computer, whether on a disk, diskette, or in RAM, for more than a very brief period of time.

Many foreign countries have additional protections which are only now emerging in the United States. The most important of these group of rights is known as the "moral rights of the author" which include the right of an author to be named as the author of a work and the right to object to use of the work which could bring dishonor or discredit on the author's reputation. These rights present particular difficulties because the Internet crosses borders. Conduct that might not be considered a violation of the moral rights of an author in the

---

[245] For questions on the different rights that the author owes on his work on the Internet, see below paragraph 4.

[246] See D. Loundy, *E-Law 2,0: Computer Information Systems Law and Operator Liability Revisited*, at http://www.eff.org/pub/Legal/e-law.paper.

[247] See T. Hardy, *The Proper Legal Regime for Cyberspace*, 55 U.P.L.R 999, 1030 (1993).

United States, for example a re-mix of a popular song, may be considered a violation in France.

2) <u>What kind of work is protected</u>?

Several works that may be found on the Internet will be examined.

a) <u>The writings</u>

* Electronic communication: Two points of view conflict. Some consider that e-mail and synchronous communications sites[248] that allow instant "live" communication between users are not protected because a transmission, in and of itself, is not a fixation.[249] A transmission may result in a fixation, but a work is not fixed by virtue of the transmission alone. Therefore, since the work is not fixed (on hard drive or diskette) at the same time as it is being transmitted, it is not be protected by the Copyright Act. The other point of view holds that, any kind of communication, even electronic is protected.[250]

However, most of the software providing electronic communication and mail automatically saves the message at the same time as it is sent. It is therefore fixed and protected and the question of copyrightability does not arise.

* Published writings: The question of protection arises if an article is directly typed and loaded in a server. However, if the author puts on the Internet an article that he has

---

[248] For example Internet Relay Chat (IRC), or Telnet.

[249] Janice R. Walker, *Protecting Cyberspace: Copyright and the World Wide Web*, 43-MAY Fed. Law. 42 (1996).

[250] Olivier Hance, *Business et Droit d'Internet*, 74 (1996) (Business and Law of the Internet).

already fixed on a paper, his work is already protected. When the article is loaded on the Internet or integrated in a web page, it is saved in the RAM and thereby fixed and protected.

b) Musical and audiovisual works

It is not because a work is put on the Internet that it loses its protection. Since musical and audiovisual works are copyrighted in the 'real world,'[251] they remain copyrighted in the cyberspace.

c) Computer programs and softwares

Computer programs, navigating on the Internet, are protected by the Copyright Act. Although section 102(a) does not expressly list computer programs as works of authorship, legislative history suggests that these programs are considered copyrightable as literary works.[252]

Such a protection is also granted to software. It has been held (again) very recently by the Court of Appeal of Ohio, in *State of Ohio v. Michael Perry*[253]. Perry without a licence from Microsoft and Clark Development Corporation, placed their software, as if it were his own, onto a bulletin board which he operated, and allowed others to use. The main issue was not whether softwares are protected, but the Court, to reach its point, stated: "We are persuaded that under the facts as stated in this case, 'copying' did occur when Perry uploaded the software onto the bulletin board."[254]

---

[251] 17 U.S.C. § 102(2)(6).

[252] See H.R. Rep. No. 1476, 94th Cong., 2d Sess. 54.

[253] 1997 WL 71299 (Ohio App. 1 Dist).

[254] Id. at 5.

In Europe a Directive of 1991, states that computer programs are protected as literary work.[255]

d) Databases

Many databases are launched on the Internet, and are often composed of uncopyrightable information.[256] Questions arise as to whether such compilations are sufficiently original and creative to satisfy the threshold requisites of copyright protection. According to the Act, where unprotectable works, data, or other information are selected, coordinated, or arranged in an original manner, the resulting compilation is protectable. [257] However, the Supreme Court in *Feist Publications, Inc, v. Rural Tel. Service Co., Inc.,* [258] ruled that a compilation is not copyrightable simply by virtue of it having required great cost and effort to arrange ("sweat of the brow" doctrine). Originality and creativity are required to make a compilation copyrightable.

This decision is very helpful to determine the copyrightability of databases in cyberspace. If the data is fact-based and presented in an obvious, mechanical, or routine way, then the compilation is not subject to copyright protection. However, if the database is

---

See also: MAI Systems Corp. v. Peak Computer Inc, 991 F.2d. 511, 517 (1993). "It is not disputed that MAI owns the copyright to the software at issue here."

[255] Directive 91/250/CEE from the council of May 14, 1991 on the Legal Protection of Computer Software, J.O.C.E., 15 mai 1991, n°L122/42.

[256] This includes fact-based information, such as demographic and statistical information, and public-domain information, such as statutes and court filings.

[257] 17 U.S.C. § 101
The Act defines a compilation as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship".

[258] 111 S.Ct. 1282 (1991). The court decided that there was insufficient creativity and originality in arranging listing in a telephone book (white pages) in alphabetical order to warrant copyright protection.

original, or the compiler derived original data from public data, the database is copyrigthtable on the Net.

In *ProCD v. Zeidenberg* [259], the District Court for the Western District of Wisconsin applied these principles to the transmission of a databases's content via the Internet. The plaintiff, ProCD, had spent several millions of dollar creating a comprehensive, national directory of more than 95 million business and residential listings, including full names, street addresses, and telephone numbers. It sold this product under the trademark "Select PhoneTM". ProCD combined the database listings and a software search engine and placed them on a CD-ROM. Along with a notice on the outside, each Select Phone package contained a single user, "shrinkwrap license"[260] agreement inside, advising that the CD-ROMs contained copyrighted material and were to be used only for personal, non commercial purposes. Defendant Zeidenberg, a computer student, purchased a copy of Select Phone. He disregarded the license agreement thinking it was not binding, and copied the contents onto the hard drive of his computer. He then created his own software search engine and made the resulting product available over the Internet World Wide Web. Zeidenberg's database was receiving approximately 20,000 hits[261] per day on the Internet. ProCD asked Zeidenberg to stop distributing the data on the Web. Because of his refusal, ProCD commenced the law suit alleging copyright infringement. The court, based on the precedent set by *Feist*[262], ruled in favor of Zeidenberg. Select Phone data, although expensive to

---

[259] 908 F. Supp. 640 (W.D. Wis. 1996).

[260] A "shrinkwrap license" is an adhesion contract that purports to take effect when the consumer opens the package and retains the goods.

[261] A hit occurs each time a new screen is displayed on a user's computer screen during a search of the database. Each search tends to generate multiple hits.

[262] See footnote 240.

compile, was not sufficiently original to merit copyright protection and thus could be copied at will.[263]

However, this decision has been overruled by the Seventh Circuit, United States Court of Appeal[264] which held that the shrinkwrap license included with software was binding on Zeidenberg, the buyer. Indeed, the software splashed the license on the screen and access is authorized only if the user accepts this license. The license will not let the user proceed without indicating acceptance. By entering the software, Zeidenberg accepts the contract.[265]

The decision of the Court of Appeal saves the companies who have developed search engines and databases of indices of Web sites, as is, for example, the case for "Yahoo!", and "Altavista". If the Court of Appeal had not overruled the District Court, an entrepreneur might have been permitted to access "Altavista" in such a way that he can effectively download the entire database of URL's from Altavista onto his own set of servers.

As it has been said, since contents on the Internet cross borders, it is important to see how the databases are protected abroad. Europe offers more protection for database owners than the USA. The directive on the Legal Protection of Databases was approved by the European Union Council of Ministers, on February 26, 1996.[266] It creates a sui generis, non right to prevent the unfair use of database contents when significant cost and efforts were expended to create it. The work is protected for a period of fifteen years[267] against

---

[263] "Plaintiff's arrangement of telephone listings lacks the minimal level of creativity necessary to garner copyright protection. Although plaintiff's software is protected by copyright law, its compiled data are not. "

908 F. Supp., at 650.

[264] ProCD v. Zeidenberg, 86 F.3d 1447 (1996).

[265] Id. at 1452.

[266] Council Directive 96/9/EC, 1996 O.J. (L.77) 20. The Directive must be implanted in national law by January 1, 1998.

[267] The right may be renewed for additional fifteen years terms if substantial changes (updates) have been made.

unauthorized "extraction"[268] or "reutilization"[269]. As the Directive defines a database[270], the protection covers virtually all material distributed via the Internet.

The Directive only protects contents of non European databases if the foreign country offers comparable protection to European databases. US database providers cannot claim this protection, since no such protection is available in the US for their European counterparts.

e) A Web page

A Web page consists of many hypertext links[271], which connect works of authorship, documents, and other hypertexts. A hypertext link is a URL[272]. A URL is a fact and therefore not protected by the Copyright Act.

The Web site in itself, the structure of the site, is not copyrightable, regardless of its originality, as it is characterized as a "method of operation."[273] This is an implication the ruling of the First Circuit in *Lotus Development Corporation v. Borland International* [274]. Borland copied the "menu tree" in the plaintiff spreadsheet program. The Court found that

---

[268] That means here "copying". The Directive, at 25-26.

[269] That means here "transmission or distribution". The Directive, at 25-26.

[270] A database is a collection of works, data, or other materials (such as texts, sounds, images and facts) arranged in a "systematic or methodical way" that is individuality accessible by electronic or other means.
Id. at 21-24.

[271] A system in which documents contain links that allow readers to move between areas of the document, following subjects of interest in a variety of different paths.

[272] Universal Resource Locator, see introduction for definition.

[273] 17 U.S.C. §102(Bb).

[274] 49 F.3d 807 (1995), aff'd by div'd ct. 116 S. Ct 804 (1996).

Borland did not infringe Lotus' copyright, because the menu command, as a "method of operation", was uncopyrightable.[275]

What is presented by the Web page, original graphics, designs, literal elements, and photographs, may be copyrightable under copyright law and trademark analysis.[276]

So, if most of the works put on the Internet may be copyrightable, an important exception is the databases, which will, most of the time, not be protected.

Except if the work is made for hire, whereupon the ownership of the work is then transferred to the employer[277], the owner of the copyright is the author. For how long is this protection granted to him?

3) The duration of the protection

a) The author is known

The protection is granted for the life of the author plus in the US a period of fifty years following his death. In Europe, the protection is granted for seventy years after the death of the author.[278]

---

[275] Id. at 818.

[276] See, e.g., Atari Games v. Oman, 979 F.2d 242 (1992), dealing with copyright on computer video games displays.

Sega Enterprises Ltd. v. Maphia, 857 F. Supp. 679 (1994), dealing with trademark infringement on video games.

[277] See 17 U.S.C. § 201 (a)(b)(c).

[278] Directive 93/98/CEE du Conseil du 29 octobre 1993 relative à l'harmonisation de la durée de protection du droit d'auteur et de certains droits voisins, J.O.C.E., 24 nov 1993, n° L290/9, art 1. (Directive to harmonize the duration of protection for copyright).

b) The author is unknown

In case of anonymous or pseudonymous works, which are common in the cyberspace, the protection is granted for seventy-five years from the date of publication of the work or one hundred years from the date of creation of the work, which ever is shorter.[279] Let's take an example. A writer writes in 1997 a poem on a sheet of paper. This poem is not publicly performed or displayed. He keeps it at home until he decides to disclose it *anonymously* to the public by the way of the Internet. The work is original, fixed on the paper, so it is copyrightable. The question that arises now is to know until when it is protected. The Act says seventy five years from the date of publication or one hundred years from the date of creation. A Publication of a work is "the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership."[280] "A work is created when it is fixed on a copy or phonorecord." [281] "Copies are material objects in which a work is fixed".[282] When the anonymous author puts his poem on the Internet, is he making a copy? Put another way, is his poem fixed on the Internet? One answered affirmatively to both questions.[283] By fixing his work, he is making a copy, and the work is therefore protected for seventy-five from the time it is put on the Internet and for 75 years. If he publishes the work on the Internet in 2007, the work will be protected until 2082, but if he publishes the work on the Internet in 2027, it will be protected only until 2097 because it is 100 years since the creation of the work (fixed on the paper), the term is shorter (2027 + 75 years = 2102).

---

[279] 17 U.S.C. § 102(a). It is also the case for a work makes for hire.

[280] 17 U.S.C. §101.

[281] Id.

[282] Id.

[283] See 1) of this paragraph.

However, many works that are *anonymously* navigating cyberspace are directly created on the Internet[284], and were not previously fixed "on a tangible medium of expression". The controversy over how long such a work is protected has not been resolved.[285] If we consider that the work is fixed when it is loaded, it is protected from the time of its creation on the Net, for one hundred years. But by launching the work on the Internet, the author is publishing it, making it available to the public. In that context, the work will be protected for a seventy year period from its protection.

As many works put on the Internet are protected by the Copyright Act, it is important to see the scope of this protection. According to § 106 of the Act,[286] the protection grants the author exclusive rights.

B) What rights are granted to the author of a work available on the Internet?

The various rights of the copyright owner will be examined first, and then we will see if these rights are enforceable in the cyberspace.

1) The rights

section 106 of the Copyright Act grants the copyright owner five exclusive rights: to reproduce the work in copies, to prepare derivative work, to distribute copies, to perform the work publicly, and to display the work publicly[287]. All of these rights can come into play in

---

[284] E.g., by electronic mail.

[285] See 1) of this paragraph.

[286] 17 U.S.C. § 106.

[287] Id.

a networked environment. If one of these rights is infringed by an Internet actor, the author may sue him for copyright infringement. The purpose of this section is to examine how the work is protected in cyberspace.

a) The right of reproduction

The owner of a copyright has the exclusive right "to reproduce the work in copies or phonorecords."[288] The right of reproduction means the right to produce a material object in which the work is duplicated, transcribed, imitated, or simulated in a fixed form from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Since this right is exclusive to the owner of the copyright, anyone who would exercise the same kind of action on the protected work would infringe the copyright.[289]

Two situations have to be studied. First, when someone loads a copyrighted work on the Internet, for example, on his Web site. And second, when an user downloads the Internet content in the RAM of his own computer to view it.

In the first situation, the issue is whether, by loading the copyrighted work on his Web page, one is reproducing the work in copies and thereby infringing the owner's exclusive right.[290] It has been said that loading a work on a Web page is 'fixing' the work. When fixing a work, one is making a copy of this work, and therefore reproducing the copyrighted work in copies. By reproducing the work in copies, the user infringes the owner's exclusive right.

---

[288] 17 U.S.C. §106.

[289] H.Rep. 94-1476 at 61.

[290] See 17 U.S.C. 106(1).

This situation is very common on the Internet[291], and how to deal with it legally is the purpose of the following section.

The second situation concerns normal usage of the Internet. Because of how the Internet works, in order to view any of the files from a network or a BBS, one must download materials into the RAM of a computer. It is impossible to read, view, listen to, print, upload, download, transfer, or otherwise access digital expression without downloading the document into the RAM.

The question that arises now, is whether the user is reproducing the work when he views it on his screen, having downloaded the work from the Internet into his RAM to view it. In other words, is downloading a work into the RAM the same as copying the work? The term 'copies' includes "material object (...) in which the work is fixed."[292] How is a work fixed? The "work is fixed (...) when its embodiment in a copy (...) is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."[293] The question that arises then, is whether or not a work is fixed when it is downloaded from the Internet into the RAM of ones computer.

This issue is very important in the domain of the Internet. Indeed, if downloading a document from the Internet is considered a fixation, the one who views a document by downloading it makes a copy and is therefore an infringer of the exclusive right of the owner to reproduce copies. Although he uses the Internet normally, the user's liability may be sought, as it has been previously explained.[294] If downloading does not constitute fixation the user will not be an infringer.

---

[291] See e.g., the 'Jacques Brel' case, infra p 86.

[292] 17 U.S.C. § 101

[293] 17 U.S.C. § 101.

[294] See chapter I, Second part.

Is a work fixed and therefore copied when the document is downloaded from the Internet into ones computer RAM? Some authors think that downloading is making copies, others disagree. Each point of view is defendable. Both opinion and their consequences will be explained. In the eyes of the Copyright Law, a user who downloads a work is legally and theorically an infringer. However, because of the nature of the Internet, surfing the web is not practically an infringement of Copyright Law.

a-1) Downloading is making copies because it is fixing the work in the RAM

This is the conclusion reached by two governmental commissions, the Commission on New Technological Uses of Copyrighted Works (CONTU),[295] and the National Information Infrastructure Task Force (White Paper),[296] issued by the Clinton Working Group on Intellectual Property.

The CONTU asserts that "the text of the new copyright law makes it clear that the placement of a copyrighted work into a computer (...) is the preparation of a copy (...). Because works in a computer storage may be repeatedly reproduced, they are fixed and, therefore, copied."[297]

According to the White Paper, copies are made whenever a digitized file is uploaded or downloaded from a user's computer to a bulletin board system or to other server, or when a file is transferred from one computer network user to another. This means that when an Internet user browses on the Web, copies of the work are temporally created and fixed in his computer memory (RAM)

---

[295] Final report issued in 1978.

[296] The Working Group published its recommendations in September 1995, in a report known as the "White Paper". Bruce A. Lehman, The Report of the Working Group on Intellectual property rights, Intellectual Property and the National Information Infrastructure (1995).

[297] CONTU Final Report at 22 (1978), reprinted in 2 Computer law § 4.04[4] at 4-317.

A number of courts has followed this ruling, holding that even temporary copies in RAM are fixed.

In *MAI Systems Corp. v. Peak Computer Inc.*[298], the plaintiff manufactured computers and created the system software for its computers. The defendant performed hardware maintenance services. The defendant's employee, in servicing customers' computers manufactured by plaintiff often turned on the customers' computers and, in so doing caused the system software to be loaded into RAM. The defendant argued that no copy of the software was made because the representation in RAM was not fixed. The Ninth Circuit held that a copy is created when a program is read into RAM[299], constituing a temporary fixation. "It supports the view that the copy made in RAM is 'fixed' and qualifies as a copy under the Copyright Act".[300] The same conclusion has been reached by the US District Court for the Northern District of California following *MAI*, in *Triad Systems Corp. v. Southeastern Express Co.*,[301] in a similar case.

According to these reports and cases, when a work is downloaded from the Internet to an user's computer's RAM, a copy is made and fixed.

In view of this, all acts such as reading e-mail, surfing the Internet, or following links or hypertext files constitute copyright infringement, because downloading a Web site and reading its contents violate the copyright holder's exclusive rights to reproduce. Therefore, the Copyright law makes surfing illegal.

This would render it impossible for a user to surf the Internet without infringing the exclusive reproduction rights belonging to the owner. It would limit opportunities for

---

[298] 991 F.2d 511 (1993), cert. dismissed, 114 S. Ct. 671 (1994).

[299] Id. at 518
"The loading of copyrighted computer software from a storage medium (hard disk, floppy disk, or read only memory) into the memory of a central processing unit causes a copy to be made."

[300] Id. at 519.

[301] 31 U.S.P.Q. 2d 1239 (1994).

progress and change by restricting access to information. It would also compel providers to ask fees to permit surfing on the Internet. This is contrary to the primary aim of the Internet; the free flow of information.

This scenario looks catastrophic, and seems to signal the end of the Internet. Fortunately, even if this approach to copyright is considered good law, the law provides ways to protect the Internet user from being considered an infringer. This will be studied in the second section on the right of the Inetrnet user.

A alternative scenario is that downloading contents does not constitute making copies.

a-2) Downloading is not making copies, because it is not fixing the work in RAM

This assertion is founded on the House Report accompanying the 1976 revision to the Copyright Act. It states that "the definition of 'fixation' would exclude from the concept purely evanescent or transient reproductions such as those projected briefly on a screen, (...) or captured momentarily in the 'memory' of a computer".[302] This view of fixation has been maintained by many authors.[303]

When a user is viewing a work on the Internet, he transmits the work into his computer by downloading the digital form of the work into the RAM of the computer. However, when he turns off the computer, or begins viewing something else, the information disappears. Has the information being 'fixed'? Fixation requires that the work be "sufficiently permanent or stable to permit [the copy] to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration".[304] As soon as the

---

[302] H.R. Rep. No. 1476, 94th Cong., 2d Sess., at 53 (1976).

[303] E.g., M. Scott, Computer law § 3.28 at 3-106 (1993),
"For a work to be 'reproduced', its fixation in tangible form must be 'sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.' Thus, the showing of images on a screen or tube would not be a [reproduction]."

[304] 17 U.S.C. §101.

contents on the screen change, the information disappears. This, therefore, does not appear to fulfill the requirement of permanence outlined by the Act.

If there is no fixation, then there is no copying and no infringement. The user can navigate and surf the Internet safely, without being accused of infringing a copyright by viewing the contents of a work.

In no cases involving the Internet directly has a court made a definitive decision about the controversy of fixation. Nevertheless, the second interpretation seems to be the more accurate one. It is indeed difficult to imagine that fixation is made on a computer RAM, when the work may disappear at any time (for example in just few second) by clicking a mouse. However, when the user prints of saves on disk or hard drive the document he is viewing, he fixes the work on a 'tangible medium of expression' and infringes the exclusive rights of the owner.

b) The right to prepare derivative works

The Copyright Act defines a derivative work as encompassing any "form in which a work may be recast, transformed or adapted."[305] This is applied in the cyberworld in the same way as in the 'real world'.[306]

c) The right to distribute copies

One question that arises in cyberspace is whether disseminating a work on a digital network only constitutes a public performance or display by means of transmission of the work, or whether it may be also considered as a distribution of copies. For example, it is very

---

[305] 17 U.S.C. §101.

[306] For example, one downloads a song and changes some of the lyrics to make a parody.

common on the Internet to forward to a third user electronic messages received in one's mailbox. For example, Steve sends a poem to Betty, this message is copyrightable because it is original and fixed onto Steve's hard drive.[307] Betty receives this poem, reads it and forwards it to Candy. She still has the message in her box because it is automatically saved. Is Betty infringing Steve's copyright of the poem? She may have infringed Steve's exclusive right to distribute copies of his work.

In the White Paper, the Working Group recommends that Congress amend the Copyright Act to include "transmissions" of works in its definition of distribution.[308] It recommends also that the definitions of "transmit" and "publication" in Section 106 of the Copyright Act be amended to include transmissions of copies of a work. [309] The transmission of a work by means of the Internet to newsgroups, third parties and forums of discussion, will legally be an infringement under such a definition.

d) The right to perform and display the work publicly

To perform a work means "to recite, render, play, dance, or act it, either directly or by means of any device or process." [310] Such devices and processes include "all kinds of equipment for reproducing or amplifying sounds or visual images, any sort of transmitting apparatus, any type of electronic retrieval system, and any other techniques and systems not

---

[307] See above first paragraph. If the poem is not saved, it is not fixed, and there is no copyright.

[308] It specifies an exclusive right to "distribute copies (...) to the public (...) by transmission."

[309] See the White Paper at 138, 141-42.
The definition of transmit would then be: "to transmit a reproduction is to distribute it by any device or process whereby a copy or phonorecord of the work is fixed beyond the place from which it was sent."

[310] 17 U.S.C. § 101.

yet in use or even invented." [311] To perform an audiovisual work means "to show its images in any sequences or to make the sounds accompanying it audible." [312]

The scope of the copyright holder's control over sound recordings has been expanded by the passage of the "Digital Performance Right in Sound Recordings Act of 1995." This Act creates a performance right in sound recordings for the transmission of certain copyrighted musical works by means of "digital audio transmission"[313]. The aim of this Act is to increase protection for this kind of work on the Internet. For example, providing a noninteractive Web page that automatically plays a sound recording is exempt. However, providing such a Web page either on a subscription basis or an interactive basis is not exempt.[314]

To display a work means "to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process or, in the case of a motion picture or other audiovisual work, to show individual images non sequentially." [315] This definition includes the showing of an image on a computer screen.

These rights of performance and display are limited to public performances. The Act provides that a work is performed or displayed "publicly" if it is performed or displayed "at any place where a substantial number of persons outside a normal circle of a family and its social acquaintances is gathered." [316]

---

[311] H. Rep. 94-1476 at 63.

[312] 17 U.S.C. § 101.

[313] See 17 U.S.C. § 106(6) "The owner of copyright under this title has the exclusive rights to do and to authorize any of the following:
(...)- in the case of sound recordings, to perform the right publicly by mean of a digital audio transmission".

[314] section 114(d)(1) of the Act.

[315] 17 U.S.C. § 101.

[316] 17 U.S.C. § 101.

In the scope of the Internet, playing sequences of audiovisual output (images and sounds), on a computer constitutes a performance or a display. The "publicly" requirement has to be fulfilled.

Some people might consider that in the "global village" of cyberspace, the entire community of network users would be considered a normal circle of family and its social acquaintances. But seriously, two performance situations may be compared. If the performance or the display is limited to a normal and usual business or friendly meeting involving a limited number of persons at a private place (a house, or association), this performance or display will be private, not public. There would be no copyright infringement when performing or displaying the work on the Internet to show it to this group. However, if the performance or display takes place in a public meeting it is likely to constitute a public performance or display, regardless to the number of persons attending. That would be the case, for example, if someone made a public announcement that he intends to display music of the Rolling Stones by the mean of the Internet.[317]

The owner of a copyrighted work navigating on the Internet has the same rights as any other copyright owner in the real world. But is it, in cyberspace, so easy for him to enforce his rights when they are infringed? When a right is easily infringed, like on the Internet, and liability is not enforceable this right is of little value.

2) Enforcement of these rights in cyberspace

The best way to enforce one's copyright is to seek liability by suing infringers for copyright violation. The liability of the actors of the Internet for copyright infringement has been explained in the first chapter, second part. We explained in this part that seeking

---

[317] It is possible to listen to their musics on their own Web site at http://www.stones.com

liability on the Internet for infringement is not easy. Users are extremely numerous, dispersed worldwide, and often anonymous.

In France, a case of infringement of copyright on the Internet has already been argued in front of a tribunal. By an ordinance,[318] on August 14, 1996, the Tribunal de Grande Instance de Paris,[319] recognized an infringement of copyright, when the work of an author was loaded on the Internet and made available to users of the Web without the authorization of the author (copyright owner). Students from three well known high schools, two in France[320] and one in Switzerland[321] had numerized and loaded on their Web site the text of part of some songs of Jacques Brel. The President of the Tribunal ordered the students to close the site carrying the infringed materials. He stressed that, by loading the work on the Internet, they did not make private use of the work but reproduced it and furthered a collective use of the work.[322]

In the US, the White Paper proposes legislation which would make it easier for copyright owner to enforce their rights on the Internet. This proposal incorporates the National Information Infrastructure Copyright Protection Act of 1995, which is currently in committee in both the Senate and the House of Representatives. The most relevant recommendations are the following:

- prohibition of any device or product whose primary purpose is to deactivate, without authorization, any technological protections which prevent or inhibit the violation of exclusive rights under the Copyright Law.

---

[318] This ordinance has not been published, but is available on the Net at http://www.celog.fr/expertises/refere.htm

[319] First degree of jurisdiction.

[320] Ecole Centrale de Paris, and Ecole nationale Supérieure des Télécommunications.

[321] Ecole Polytechnique Fédérale de Lausane.

[322] What is forbidden by article L. 122.5.2 du Code de la Propriété Intellectuelle. (Intellectual Property Code).

- prohibition of the distribution of copyright management information that is known to be false as well as the unauthorized removal or alteration of copyright management information (such as name or other identifying information of an author or copyright owner, or the terms and conditions for the uses of the work).

- support of an amendment to the Copyright Law and the Criminal Law which makes it a criminal offense to willfully infringe a copyright by reproducing or distributing copies with a retail value of $5,000 or more.

The rights of the author, the copyright owner, have been defined. Given these rights, what is the Internet user allowed to do? What are his rights?

II) WHAT ARE THE RIGHTS OF THE INTERNET USER?

As has been explained, the Internet user, by loading or viewing contents on the Internet, will infringe the copyrght owner's rights. However, in some situations, the user will be able to avoid the copyright infringement and defend his right to use the Internet freely. The body of rights of the user is established by the Law, and by agreement.

A) The legal rights of the user: the fair use doctrine

According to the "fair use doctrine", there is no infringement of the exclusive rights of the copyright owner if the use of the copyrighted work, including the reproduction of the work in copies, is "for purposes such as criticism, comment, news reporting, teaching (...), scholarship, or research." [323] To determine the fair use, the courts have to consider four factors:

---

[323] 17 U.S.C. §107.

- the purpose and character of the use (e.g., use of commercial nature or for non profit educational purposes);

- the nature of the copyrighted work;

- the amount and substantiality of the portion used in relation to the copyrighted work as a whole;

- the effect of the use upon the potential market for or value of the copyrighted work.

Fair use is the defense that most defendants, in cases of copyright infringement on the Internet, must argue. Fair use arguments will be based on the fact that their use of the protected work was personal, with no public or commercial purpose. A personal use is "the private use of a work for one's learning, enjoyment, or sharing with colleague or friend (...) without any motive for profit."[324] Many, if not most, users who access protected work through the Internet simply to view it, do not seek to compete with the copyright owner by commercializing or engaging in further reproduction and dissemination of the work.

Opponents of the claim of fair use on grounds that the use is personal argue that even private noncommercial copying provides the user with the benefit of a copy for which they have not paid. More over, substantial harm can result to the market value of the work. Indeed, if a work may instantly be accessed for free on the Web, potential users of the work will have no incentive to pay the copyright holder for the same access.[325]

The US has not traditionally included a general 'private copying' exception in copyright legislation. However, in 1984, the Supreme Court employed implied license and economic insignificance justifications to create a limited private copying exception, which

---

[324] L. Ray Patterson & Stanley W. Lindberg, The Nature of Copyright, A Law of Users' Rights 193 (1991), at 11,12.

[325] This argument has been sustained by the court in *Sega Enterprises Ltd. v. Maphia* (cf supra footnote 209) to reject the defendant fair use argument. The court noted that if such copying were to become widespread, it would have a substantial adverse effect on the market for the plaintiff's games. Sega Enterprises Ltd. v. Maphia, 857 F. Supp. 679 (1994), at 668.

presume that private noncommercial copying is fair use. In the *Sony* [326] case, which involved video taping, the Court held that because the public had been "invited to witness (...) [the program in its] entirety free of charge," [327] copying it for time-shifting purposes was a "fair use" of the copyrighted work.

In addition, the White Paper, in its proposal, states that, to be an infringement, the distribution must be a distribution to the public.

To apply the theory of fair use to the Internet, one has to consider separately the issue of infringement on the Web and on the e-mail.

* "Fair use" defense for the Web user.

It can be assumed that, when the Internet user is viewing contents on the Internet, he is copying the copyrighted work for his personal, private use. This is a fair use of the work, and no infringement is committed.

It is be more difficult to maintain the same argument in cases of copyrighted work being loaded by people other than the author of the work on the network. In such a case, the purpose of the use is not private but destinated for the public. The work is loaded to be viewed by a great number of people worldwide. More over, the use in such a case is often commercial, such as when the work is loaded by a commercial online provider which charges a fee for viewing the work. The fair use doctrine does not apply in such case.

* "Fair use" defense for the e-mailer.

If someone accesses a document on the web and e-mails it to himself or to someone else, has he violated copyright laws? This distribution of the work is a personal use and the work will not be distributed to the general public. The use of the work is private. There is no

---

[326] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[327] Id. at 449.

broad distribution. More over, the White Paper states that the transmission of a copyrighted work from one person to another in a private e-mail message does not constitute a distribution to the public, and therefore does not constitute an infringement.

One may sometime wonder whether e-mail is as private as it aims to be,[328] but since it is not the purpose of e-mail to be viewed by anyone else than its proprietor, the fact that illegally (by hackers) or legally[329] people may access another's e-mail does not make it public.

The fair use doctrine makes a special exemption for libraries and educational uses of works. Many universities have already moved to cyberspace and opened their own Web site, providing materials and distance learning. Does posting course materials on a class Web page for access by students all around the world constitute copyright infringement? These issues have still to be resolved. The White Paper proposes to expand such exemptions to take digital technology into account. The legislation would also allow libraries to make digital copies of their holdings for purposes of preservation. The other body of rights belonging to the user of the Internet are the contractual rights

B) <u>The contractual rights of the user</u>

A user of the Internet must seek the authorization of the copyright owner to be able to use his work.The user is best protected from liability by having the express authorization,

---

[328] See, Eryn Brown, *Who's reading your e-mail? It could be anybody. A competitor. Your boss. Or the hackers we hired to show how easy it is,* FORTUNE, February 3, 1997. p 56. Eryn Brown in his article even asserts: "Never expect privacy for E-mail sent through a company system", p66.

[329] The Tampa Tribune, Nov. 9, 1995, p.7.
For example, all university server are considered state property, and all messages thereon are saved on tapes, and liable to review in cases when it is determined that untoward activity has taken place. Recently, for example, a former of the University of South Florida was suspected of terrorism activities and the tapes concerning his e-mail were subpoaned.

from the copyright owner, but sometimes, the authorization is only implied by the conduct of the copyright owner through the normal use of the Internet.

1) An express authorization

Express authorization may be established in a contract or by a notice on the work.

a) By a contract: the license

The US Copyright Act provides that authors may transfer their rights of copyright in whole or in part, but a grant of exclusive rights must be made in an "instrument of conveyance, or a note or memorandum of the transfer (...) in writing and signed by the owner of the rights conveyed." [330]

A license is a good means to bind the server. Before copying the work on his Web site, the server must first obtain from the author the authorization to reproduce and distribute copies of the work. With this license, he will not infringe the rights of the copyright owner.

It will, however, be very difficult to bind the ultimate Internet user (the one who is viewing the work by downloading it on his computer RAM) with a contract because users are so numerous scattered around the world. Copyright owners will therefore have to try to prevent the Internet user from improperly usimg his work, by including as part of the home page a stated restriction on the downloading and reuse or retransmission of the Web site materials. This is typically done through a license agreement that purports to bind final users who access the site. For example, on the home page, the copyright owner could write: "The materials you are about to view on this site are protected by the Copyright Law. By clicking HERE you agree not to infringe the exclusive rights of the copyright owner: to reproduce the

---

[330] 17 U.S.C. 204(a).

materials in copies, to prepare derivative materials, to distribute the materials, or to perform or display the materials publicly. You are allowed only to make copies for your personal use. Any commercial use of the content of this site is forbidden." More sophisticated "point and click" contracts require an end user to register by name (and even password), and to click on an icon that records his agreement to the license restrictions governing the use of materials on the site before receiving full access to the site.

This kind of license has been applied by the Seventh Circuit Court of Appeal.[331] According to this decision, by clicking, the user agrees with the terms of the contract and accepts the license.

Many copyright owners leave the task of monitory users to the access provider. Since online providers control the physical access to the works, they can make access contingent upon accepting the terms of their license. This is, for example, what American On-Line does, subjecting any use of its services to a prewritten license.[332]

To bind the Internet user, a notice by the copyright owner is also sufficient.

b) By a notice

The proper form of a copyright notice consists of the word "Copyright", or the abbreviation "Copr.", or the more familiar © followed by the year in which the work was published, followed by the name of the copyright owner.[333] If there is such a notice on a

---

[331] See supra footnote 264.

[332] This license states in the part dealing with Proprietary rights: "All content is copyrighted as a collective work under the US Copyright Laws, and AOL Inc. owns a copyright selection, coordination, arrangement and enhancement of such content. Members may not modify, publish, transmit, participate in the transfer or sale, create derivative works, or in any way exploit any of the content, in whole or in part. If no specific restrictions are displayed, members may make copies of portion content, including copyrighted material, trademarks, or other proprietary materials, provided that the copies are made only for member's personal use."

[333] E.g., Copyright © 1996 by the State Bar of Wisconsin, All rights reserved.

work, the viewer of the work is assumed to be aware that the work is copyrighted. This notice can prevent a third party from later claiming that any taking of the protected work was innocent infringement.

For this reason, copyrighted work made available on the Internet should be accompanied by a notice of copyright. The final user knows that the work is not freely available, even if it is launched on the Internet. With the notice, the copyright owner warns that his work is protected, and that copying it will be an infringement, that may result in a legal suit.

Following the notice, the copyright owner, may also specify to what extent his work may be exploited by a user. For example, two types of authorization exist for software: shareware and freeware. In the case of shareware, the copyright owner on the software allows anyone on the network to load the software and to try it for a while. If he wants to keep it, the user will have to pay fees to the copyright owner, otherwise he will infringe the rights on the work. It is a good means for an author of software to distribute his work on the network. In the case of freeware, the user does have to pay a fee at the time of loading the software.

Nevertheless, what prevents the Internet user from being an infringer of the right of the copyright owner, while navigating the Web, is the authorization that the copyright owner implicitly grant to use the work.

2) An implied authorization

The Internet user may be protected from infringing copyright while navigating the Web by the implicit authorization the copyright owner has granted to use the work when the owner loaded the work onto the Net.

It has been argued that, the simple fact of viewing content on the Internet, can be considered an infringement of copyright because, while viewing, the Internet user fixes a copy of the protected work in the RAM of his computer. However, when a copyright owner

decides to load his protected work on the Internet, he presumably wants to diffuse his work, to make it knowed to a great number of people, all around the world. He knows that his work will navigate, and that he risks losing supervision and management of the diffusion of the work. Because it is generally known that much information is freely available on the Internet, the user may be considered to have an implied license to view the work or even download a copy. The survival of the Internet requires that this implied license exist. Without any implied license, everyone connecting to the Internet would be an infringer. It is not the purpose of the copyright owner, when he makes his work freely available on the Internet, to make the user an infringer.

Every user should follow the Internet code (netiquette), and make fair use of the content available on the network. This is a consensus between each actor in cyberspace, because it is in their best interest that the Internet remain a free medium to send information on any topic everywhere, and to view the information from anywhere.

In case of doubt, one who wants to load a work on the Internet, or download it for any other use than fair use, should obtain an explicit authorization from the author to use the work, thereby avoiding any kind of liability.

SECOND PART: PROTECTION GRANTED BY THE FREEDOM OF SPEECH PRINCIPLES

The main purpose of the Internet is to permit an international free flow of information on any subject or topic. This free flow of information is, in many countries, legally guaranted and called the freedom of speech.[334] In the United States, this freedom of speech is guaranteed by the First Amendment of the Constitution. Different mediums, such as

---

[334] See chapter I, first part.

writings, pictures, designs, or sounds, carry information on the network, all over the world, and are all protected under freedom of speech. Anyone may express his point of view, freely writing or showing images topic over the Internet. The user, by loading content on the network, is sure to reach a great many people all over the world. More over, he can anonymously load any kind of material on the Internet without risking that the information will be traced back to him.

That is the reason why sites providing sexually explicit material or other illegal contents are flourishing on the network. Does the First Amendment allow flow of any kind of information on the Internet? Is it permitted by the First Amendment to load obscene stories or pictures on the Internet?

These questions may be answered by considering first obscene material on the Internet, and second other reprehensible conduct.

I) The First Amendment with regard to obscenity on the Internet

The First Amendment guarantees the free flow of information and freedom of speech on the Web and on the electronic mail (e-mail), just as in a newspaper, or on TV or radio. Everyone has the right to express themselves and give their point of view on any topic.

The US Government, afraid of the growth of obscene and sexually oriented Web sites[335] has enacted, in 1996, the Communication Decency Act, to limit the transmission of obscene material over the Internet.

A quick background on the history of the First Amendment towards obscene and indecent speech is necessary for a better understanding of the Communication Decency Act.

---

[335] See e.g., http://www.nude.com

A) Background on the regulation of obscene and indecent speech

Obscene materials have historically been subject to statutory prohibition and do not receive First Amendment protection. Since *Commonwealth v. Sharpless,*[336] the American judicial system has consistently held that obscenity falls outside the protection of the First Amendment.[337] Nowadays, courts use three criteria to determine whether a work is obscene: whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; whether the material depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable law; and whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[338] The distribution or public exhibition of sexually explicit work that meets the *Miller* definition for obscenity may today constitutionally be banned, whether the alleged obscenity is printed, broadcasted, mailed, distributed by telephone, or made available on the Internet. The courts have defined what constitute "patently offensive" material[339] and has held that a statute must clearly define what is patently offensive to withstand constitutional challenge.[340]

Indecent material that does not reach to the level of obscenity, is however protected under the First Amendment, albeit to a limited degree. Under the "captive audience

---

[336] 2 S.R. 91 (1815).

[337] E.g., Roth v. United States, 354 U.S. 476 (1957).

[338] See Miller v. California, 413 U.S. 15, 24 (1973).

[339] Miller, 413 U.S., at 25.
Material will be deemed patently offensive if it represents or depicts "ultimate sexual acts, normal or perverted, actual or simulated; masturbation; excretory functions; or lewd exhibition of the genitals."

[340] Id.

doctrine,"[341] if the viewer can avoid the indecent expression, the First Amendment right to freedom of expression will prevail. However, in *FCC v. Pacifica*, the Supreme Court held that regulation of indecent material is justified when it prevents children's exposure to offensive expressions.[342] The Court held, further, that for a statute to regulate indecent material, the regulation must be narrowly tailored to serve the government's purpose of preventing exposure to minors or unwilling recipients.

The telephone and television are the two mediums of communication that have traditionally been refgulated with respect to the First Amendment.The telephone 'dial-a-porn' industry became regulated in 1983 when §223 of the Communications Act of 1934 was amended to prohibit the making by telephone of "any obscene or indecent communication for commercial purposes to any person under the age of eighteen or to any other person without that person's consent." [343] In *Sable Communications of Cal. v. FCC*[344], the Court pointed out the difference between obscenity and indecent communications with regards to the protection by the First Amendment: "Sexual expression which is indecent but not obscene is protected by the First Amendment."[345] The Court held that "the Government may regulate content of constitutionally protected speech in order to promote compelling interest if it chooses the least restrictive means to further articulated interest."[346] The 'least restrictive mean' may, for example, be an age verification by the use of a credit card.

---

[341] Erznoznik v. City of Jacksonville, 422 U.S. 205, 209 (1975).

[342] 438 U.S. 726, 732 (1978).

[343] 47 U.S.C. 223(b) (1983).

[344] 492 U.S. 115 (1989).

[345] Id. at 125.

[346] Id. at 126.

In the context of the cable television industry, the same test of "least restrictive mean" applies[347] to regulation of freedom of speech.

Though the Internet has many similarities to these mediums of expression important differences exist[348] that have compelled compelling the Government to enact a new law, adressing Freedom of speech in this new medium, the Communication Decency Act.

B) The Communication Decency Act[349]

The Communication Decency Act (CDA) is part of the 1996 Telecommunication Act, which was enacted on February 8, 1996. The CDA establishes the criminal liability of people who use or allow the use of telecommunications devices for knowing transmission of "indecent" communication to minors, and who use or allow the use of "interactive computer services" to display communication to minors depicting or describing sexual activities in "patently offensive" ways.[350] The CDA also criminalizes, through its amendment of 18 U.S.C. §1462(c), transmission by telecommunications devices of information about abortions or abortifacient drugs and devices. This amendment apply of course to the Internet, because it is a telecommunications device.

The constitutionality of these provisions was challenged in the courts at the time the CDA was enacted. The first decision, *American Civil Liberties Union v. Reno*[351] was made

---

[347] See United States v. O'Brien, 391 U.S. 367 (1968).

[348] Whereas a dial-a-porn provider has the technology available to ascertain the community from which incoming calls are made, no such technology is available to the access provider. Since the accessibility to a service provider, the access provider has no awareness of the communities from which accessors of his service originate.

[349] 47 U.S.C. § 223 et seq.

[350] See 47 U.S.C. 223(a), 223(d), 223(a)(1)(B), 223(d)(1), 223(a)(2), 223(d)(2).

[351] 929 F. Supp. 824 (1996).

by the United States District Court for the Eastern District of Pennsylvania, and the second, *Shea v. Reno,* [352] by the United States District Court for the Southern District of New-York. The plaintiffs, in both cases sough to prove that the provisions of the CDA are unconstitutional and contrary to the principle of freedom of speech of the First Amendment. It is not possible, on the Internet, to be sure of who, minor or adult, is viewing content. To prevent minors from downloading indecent content off the Web, providers would have to preclude any such content from being loaded on the network.

By banning the exposure of obscene and indecent speech to minors, the CDA renders access to these materials by adults impossible. But indecent materials are protected by the First Amendment. The plaintiffs argued that the CDA violates the First Amendment because it effectively bans a category of protected speech from most parts of the Internet.
The issue then became what the effect of the CDA was on the free availability to adults of constitutionally protected material. The Government maintained that the CDA does not in word or in action, ban indecent material that is constitutionally protected from adults.

The District Court ruled that "the CDA reaches speech subject to the full protection of the First Amendment, at least for adults"[353] On the WWW it is technically feasible, through the use of Common Gateway Interface scripts, to verify the age of a user. [354] However, in practise, non-commercial organizations and even many commercial organizations (such as Prodigy, CompuServe, America Online) would find it prohibitively

---

[352] 930 F. Supp. 916 (1996).

[353] 929 F. Supp, at 855.

[354] Id. at 845.
"An HTML document can include a fill-in-the-blank "form" to request information from a visitor to a Web site, and this information can be transmitted back to the Web server and be processed by a computer program, usually a Common Gateway Interface (cgi) script. The Web server could then grant or deny access to the information sought. The cgi script is the means by which a Web site can process a fill-in form and thereby screen visitors by requesting a credit card number."

expensive[355] and burdensome to engage in age verification proposed by the government. More over, even if they attempted to verify age, there is little assurance that they could successfully filter out minors. There is no effective way for many Internet content providers to limit the effect of the CDA only to minors, because there is no realistic way for many providers to ascertain the age of those accessing their materials.

The Court concluded that "it is either technologically impossible or economically prohibitive for [on-line provider] to comply with the CDA without seriously impeding their posting of online material which adults have a constitutional right to access."[356]

The Court then held that the word "indecent" is unconstitutionally vague, and that the terms "in context", and "patently offensive" also are so vague as to violate the First and Fifth Amendments. The CDA was found to be unconstitutional to the extent that it prohibits indecency and thereby violates the First Amendment. *ACLU* and *Shea* are pending appeal before the Supreme Court.[357]

The CDA also applies to the electronic-mail (online telecommunication). The difference with e-mail is that, when someone writes a message and sends it, he knows to who he is writing this message. The message has a known destination. This may seem to simplify the issue of applicability of the CDA. However, even if the sender knows who the recipient is, he may not know how old he/she is. It is not possible for senders to conduct age screenings. Therefore, in order to apply the CDA, the senders would have to restrict their communication to that which is appropriate for children, in order to avoid violating the

---

[355] Id. at 846.
The cost of a credit card verification is $1 per verification. For example, Critical Path received 3,300 hits daily from February 4 through March 4, 1996. If Critical Path must pay a fee every time a user initially enters its site, then, to provide free access to its non commercial site, it would incur a monthly cost far beyond its modest resources.

[356] Id. at 854.

[357] See the briefs: Reno v. American Civil Liberties Union, 117 S. Ct. 1241 (1997).
It should be decided in July, 1997.

statute. This would effect a complete ban, even for adults, of "indecent" expression, to which they are entitled.

We face with e-mail the same problem as with the Web, which leads also to the unconstitutionality of the CDA.

The CDA has been cited one time in a case dealing with the Internet, to affirm that it preempts state law. The Court held that state law, which prompted action against an Internet service provider for negligently permitting dissemination of defamatory statements on its bulletin board, is preempted as in conflict with 1996 CDA provision barring treatment of such providers as publishers or speakers, 47 U.S.C. 230(c)(1), and is in conflict with the CDA's purpose of blocking the dissemination of objectionable material by such providers.[358]

Obscene and sexually oriented speech is not the only regulated type of speech. Other reprehensible conduct are not protected by the First Amendment.

II) The First Amendment toward other reprehensible conduct on the Internet

The First Amendment protects only speech not forbidden by the law. Unlawful speech is not protected and its author may be punished.

In the United States, the U.S. Code, prohibits communication containing a threat to kidnap or injure an individual.[359] In 1994, two students (Baker and Gonda) exchanged, via e-mail, messages describing the torture, rape, and murder of a young woman who shared the name of one of Baker's classmates at the University of Michigan. Baker was arrested in 1995 and a federal grand jury returned a one-count indictment, charging Baker for violation of 18 U.S.C. § 875(c). The District Court dismissed the indictment against Baxter, reasoning that

---

[358] Zeran v. America Online Inc., 1997 WL 135703 (E.D. Va).

[359] 18 U.S.C. § 875(c).

the e-mail messages sent and received by Baxter and Gonda did not constitute a "true threat"[360] under the First Amendment and, as such, were protected speech."[361]

In cyberspace, the First Amendment protects and forbids the same speeches than in the real world. Religious opinion is protected while extremist propaganda is forbidden.[362] The Internet must be an open medium, but it cannot function outside the law. In Germany, for example, the head of CompuServe's German operations was charged in April with distributing illegal pornography and neoNazi materials.[363] He was held criminally liable for enabling subscribers to gain access to material banned by local laws. The Munich Office, one of the few full-time Internet patrols, uncovered 110 postings of illegal material in 1996, two-thirds involving material from outside Germany.

Transmission of information in cyberspace via the e-mail raises specific First Amendment issues. Does the First Amendment gives one the right to send messages to someone else, even if he refuses to receive these messages? Does the receiver infringe the sender's First Amendment's right when he prevents these messages from reaching his e-mail address?

Several Courts have addressed these questions[364]. They all came to the same decision. In *Cyber Promotions Inc. v. America Online Inc.*[365] the issue was whether, under the First Amendment, one private company has the unfettered right to send unsolicited e-mail advertisements to subscribers of another private online company over the Internet and

---

[360] With the intend to realize a specific purpose trough intimidation.

[361] United States v. Baker, 890 F. Supp. 1375, 1381 (1995). The United States Court of Appeal affirmed: 104 F.d. 1492 (1997).

[362] E.g., incitement to racial hatred. Notice that it is not the case in the United States.

[363] CompuServe has already been compelled to close in 1995, 200 Internet discussion newsgroups found to be offensive or illegal by the Bavarian authority.

[364] See e.g., CompuServe Inc. v. Cyber Promotions Inc., 1997 WL 109303 (S.D. Ohio).

[365] 948 F. Supp. 436 (1996).

whether the private online company has the right to block the e-mails advertisements from reaching its members. In that case, Cyber Promotion (CP) sent e-mail advertisements to American Online (AOL) subscribers, who complained about these e-mails. AOL practiced "e-mail bombing" to protect its subscribers. It set all unsolicited e-mails sent by CP to undeliverable addresses, altered their return paths, and then sent them back to CP. The Court concluded that the First Amendment does not give CP the right to send unsolicited e-mail to AOL's subscribers. More over, AOL is a private entity and its conduct does not have the character of a state action, therefore, AOL does not violate CP's First Amendment right by blocking CP's unsolicited e-mails from reaching its subscribers. CP is only protected against public action to prevent the transmission of the works. It is not possible to demand this protection against a private entity who would block the communication, unless this private entity's conduct has the character of state action.[366]

---

[366] As a general matter, private action can only be considered state action when there is a sufficiently close nexus between the state and the challenged action of the private entity so that the action of the latter may be fairly treated as that of the state itself. There are three distinct tests in this context. First, courts must consider whether the private entity has exercised powers that are traditionally the exclusive prerogative of the state. If it does not exercise such powers, the court must consider whether the private entity has acted with the help of, or in concert with state officials. The final test is whether the state has so far insinuated itself into a position of interdependence with the acting party that it must be recognized as a joint participant in the challenged activity.

948 F. Supp., at 441, quoting: Blum v. Yaretsky, 457 US 991 (1982), and Marck v. Borough of Hatboro, 57 F.d. 1137, 1142 (1995).

CONCLUSION

This conclusion will summarize the main issues of this thesis so as to draw briefly a legal regime of the Internet, helpful for the current and future Internet users. Each point will be analyzed to see if the law really fits the reality and the original purpose of the cyberspace. It will be finally asserted that the Internet does not need the enactment of new laws, but self regulation.

Preexisting laws and newly enacted laws can be applied to the Internet to fill the so called "no law land" which so many people were afraid of. There is law on the Internet which every user, is expected to follow. However, because of the international aspect of the Internet, and because it is sometimes impossible to trace people loading content on the network, it is often impossible to enforce these rules. Who is he and where is he? Also, which nation's laws apply to him, and how can he be bound by a foreign court's decision? The law will require the help of advanced technology to fight against wrongdoers. Police will have to use computer technicians and high-performance computers to look for illegal behavior in closed and protected web rooms. Everyone will have to adapt to the emergence of this new world, the cyberworld.

Because the main author of the illegal action will be difficult to find, liability and remedy will often be sought against the visable part of the iceberg: the Internet Service Provider (ISP). The level of liability of the ISP will depend on its relationship to the content it is asked to load. In cases of defamatory or obscene statements, the ISP is considered merely a distributor if it has no more editorial control over publication than does a public library. The distributor does not know, and has no reason to know, of the allegedly defamatory statement. In such a case, the ISP cannot be held liable for any defamatory or obscene

message sent through its service. However, if the ISP is considered a publisher, if it controls the content of the messages posted on its service and is expected to be aware of the defamatory or obscene statement, it can be held liable for publishing the material.[367]

The liability of the ISP can also be sought by a copyright owner, who discovers that his is protected work is being distributed on the Internet without his authorization. His claim will succeed if he can show a direct or contributory infringement from the ISP.

The fact of ISP liability raises a lot of questions and problems. If the ISP's liability reaches a high level, they will have to take on insurance to protect themselves. The fees to use the Internet would be expected to rise proportionally. But the main purpose of the Internet is to provide a lot of information at a low price, and to permit people to communicate freely and easily all over the world. Huge fees will certainly divert the Internet from its original goal, and risk destroying it. More over, it is technically very difficult for an ISP to control the millions of materials posted through it every day on the Internet. ISPs would have to be equipped with very expensive devices to monitor located content, which would, here again, increase the fees of each user.

The other, and even more important, problem of such a control concerns the freedom of speech. Has an ISP the right to control materials and decide, on its own, what is defamatory, indecent, or obscene? Is it the role of the ISP to be the police of the Net, and deny access to what it considers "bad"?

The Internet is a place where everyday, intentionally or not, copyright infringement occurs. The Internet is certainly the most important means of communication permitting copyright infringement. It is, also, paradoxically, the place where copyright owner's rights are the least protected and enforced.

It is regrettable that an exclusive right is infringed when someone loads onto the Internet another's work, without his authorization for the loader's to reach his own purposes.

---

[367] The standard of liability is negligence rather than strict liability.

However, inevitably, when a copyright owner decides to launch his work on the wild network, his exclusive rights will be occasionally infringed upon.

Freedom of speech is one of the most basic and important human rights. It is the foundation of every democracy, and every year people die fighting for it. It is also, certainly, the most important right of an Internet user. It protects the user from any government's intent to limit his speech. It allows Internet users to exchange freely their point of views, to tell and show many things to a wide range of people.

However, a border between what is allowed and what is not must be established. Indeed, the great opportunities offered by the Internet to easily reach people all around the world become very dangerous when the purpose of the user is criminal. The recent case of the "Heaven's Gate" web site, is a sad example of a dangerous utilization of the Net.[368] This kind of conduct has to be strongly prosecuted and sentenced by the public opinion.

The United States has been very concerned with pornography and other kinds of obscene material on the Net. The recent Communication Decency Act and the decision held by the District Court of Philadelphia[369] are proof of the Government's and the people's interest in this topic. A statement by President Bill Clinton after the decision of the District Court is revealing:

> "I remain convinced, as I was when I signed the bill, that our Constitution allows us to help parents by enforcing this Act to prevent children from being exposed to objectionable material transmitted through computer networks. I will continue to do everything I can in my Administration to give families every available tool to protect their children from these materials."[370]

---

[368] The Heaven's Gate site invites Netizen to "leave this world", and in the beginning of April 1997, 39 persons followed the instructions and committed suicide.
See NEWSWEEK, April 7, 1997, at. 26.

[369] See supra, chapter II, Second part.

[370] Statement by the President, The White House, Office of the Press Secretary, June 12, 1996. Available at http://www.cdt.org/ciec/decision_PA/960612_Clinton _stmnt.html (1996)

Is the problem of pornography on the Internet so serious that regulation is required? The kind of material available on the Internet has been accessible for years on television and in bookstores. Interdiction to buy pornographic magazines in bookstores has never preclude a teenager from getting one through friends. Examples of regulations for the protection of minors that do not work are the restrictions on cigarettes and alcohol sales.

Although there are circumstances in which restrictions on expression are permissible, and even recommended,[371] in general, the First Amendment is best served when such restrictions are kept to an absolute minimum. Each indivudual should decide for himself which ideas and beliefs are worthy of his time and interest. Each individual should decide what he wants to watch or not. Citizens may protect themselves from unwanted indecent material.[372] Besides, it is often when something is forbidden that people make the most effort to see it, to know what it is.

Governments do not need to enact radically new laws to regulate the Internet. First, because existing rules can be applied to the Internet, and second (and this is the main reason), because the Internet is an area that is already effectively self-regulated. Everyone wants the same thing, a free and relatively safe new medium of communication and information. The Internet has already a self-regulation mechanism in place, through netiquette, an unwritten code of protocol and social pressures. Violations of netiquette are often greeted with net wide admonitions in the form of flames.[373] The users, rather than judges and legislators, are the ones who best understand how to respond to problems on the Net.

---

[371] E.g., incitement to racial hatred, racism speech, trade of child pornography.

[372] The initiation of pass codes and blocking devices for parents to install into their computers will protect children without infringing on adult's First Amendment rights to enjoy whatever speech they desire.

[373] Advertisements, and even possible close of the site.

BIBLIOGRAPHY

I) General materials

- OLIVIER HANCE, LAW AND BUSINESS OF THE INTERNET (Best of Edition eds., 1996).

- EDWARD A. CAVAZOZ and GAVINO MORIN, CYBERSPACE AND THE LAW (The MIT Press eds., 1994).

- THE LAW OF CYBERSPACE (The University of Chicago eds., Legal Forum, Volume 1996).

- HENRY H. PERRIT, JR., LAW AND THE INFORMATION SUPERHIGHWAY, Willey Law eds., 1996.

- http://www.argia.fr/lij/

- http://www.grolier.fr/cyberlexnet

- http://www.calvacom.fr/jurisnet/

- http://www.findlaw.com

- http://www.lawinfo.com

- http://www.law.indiana.edu/law/v-lib/lawindex.html

- http://www.law.cornell.edu

- http://hg.org/hghome.html

II) Specific materials

Chapter I: Regulation of the Internet

First part: The relevant rules

- Trotter Hardy, *The Proper Legal Regime For "Cyberspace"*, 55 U. Pitt. L. Rev. 993 (1994).

- Henry H. Perrit, Jr., *Jurisdiction in Cyberspace*, 41 Vill. L. Rev. 1 (1996).

- Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 Vand. J. Transnat'l L. 75 (1996).

- Anne Meredith Fulton, Cyberspace and the Internet: Who Will Be the Privacy Police?, 3 CommLaw Conspectus 63 (1995).

- Amy Knoll, *Any Way But Loose: Nations regulate the Internet*, 4 Tul. J. Int'l & Comp. L. 275 (1996).

- Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SCCHITLJ 403 (1996).

- Frédéric Olivier & Eric Barbry, *Le droit des Autoroutes de l'Information et du Multimédia: un Nouveau Défi*, http://www.iway.fr/groupecx/uae/Olivier-Barbry.html (1996).

- Pierre-Yves Gautier, *Du Droit Applicable dans le "Village planétaire", au Titre de l'Usage Immatériel des Œuvres*, Recueil Dalloz, 16e cahier-chronique (1996).

- Nancy E. Muenchinger, *Le Droit Français du Multimédia et des Télécommunications*, Gaz. Pal. P. 14 (jeudi 4 avril 1996).

Second part: The liability of the actors of the Internet

- Maurits Beerepoot, *Liability of Access and Service Providers for Online Content*, http://www.iway.fr/groupecx/uae/Beerepoot.html (1996).

- Giorgio Bovenzi, *Liabilities of System Operators on the Internet*, 11 Berkeley Tech. L.J. 93 (1996).

- Joseph N. Campolo, *Establishing Liability for On-Line Service Providers*, 6 FDMIPMELJ 721 (1996).

- Yaman Akdeniz, *Recent Developments on UK and US Defamation Law Concerning the Internet*, http://www.argia.fr/lij/english/ArticleJuin96-1.html (1996).

- Matthew C. Siderits, *Defamation in Cyberspace: reconciling Cubby, Inc. v. CompuServe, and Stratton Oakmont v. Prodigy Services Co.*, 79 Marq. L. Rev. 1065 (1996).

- Richard P. Herman II, *Note and Comment: Who is Liable for On-Line Libel?*, 8 St. Thomas L. Rev. 423 (1996).

- Cynthia L. Counts & C. Amanda Martin, *Libel in Cyberspace: A Framework for Addressing Liability and Jurisdictional Issues in this New Frontier*, 59 Alb. L. Rev. 1083 (1996).

- Marc L. Caden & Stephanie E. Lucas, *Accidents on the Information Superhighways: On-Line Liability and Regulation*, 2 Rich. J. L. & Tech. 3 (1996).

- Jeffrey M. Taylor, *Liability of Usenet Moderators for Defamation Published by Flinging the Law of Defamation into Cyberspace*, 47 Fla. L. Rev. 247 (1995).

- Mark C. Morril and Sarah E. Eaton, *Protecting Copyrights On-Line: Copyright Liability for On-Line Service Providers*, 8 NO. 4J. Proprietary Rts. 2, (1996).

- John Carmichael, *In Support of the White paper: Why Online Service Providers should not receive Immunity from Traditional Notions of Vicarious and Contributory Liability for Copyright Infringement*, 16 Loy. L.A. Ent. L.J. 759 (1996).

LAW LIBRARY
UNIVERSITY OF GE

- Edward A. Cavazos and G. Chin Chao, *System Operator Liability for User's Copyright Infringement*, 4 Tex. Intell. Prop. L.J. 13 (1995).

- Andrea Sloan Pink, *Copyright Infringement Post Isoquantic Shift: Should Bulletin Board Services Be Liable?*, 43 UCLA L. Rev. 587 (1995).

Chapter II: Legal use of the Internet

First part: Copyright issues

- Paul Edward Geller, *Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World*, 20 CLMVJLA 571 (1996).

- David J. Loundy, *Revising the Copyright Law for Electronic Publishing*, 14 JMARJCIL 1 (1995).

- Benjamin R. Kuhn, *A Dilemna in Cyberspace and Beyond: Copyright Law for Intellectual Property Distributed Over the Information Superhighways of Today and Tomorrow*, 10 Temp. Int'l & Comp. L.J. 171 (1996).

- Jonathan Evan Goldberg, *Now That the Future Has Arrived, Maybe the Law Should Take a Look: Multimedia Technology and Its Interaction With the Fair Use Doctrine*, 44 Am. U.L. Rev. 919 (1995).

- Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 Colum. L.Rev. 1466 (1995).

- Niva Elkin-Koren, *Cyberlaw and Social Change: A democratic Approach to Copyright Law in Cyberspace*, 14 Cardozo Arts & Ent. L.J. 215 (1996).

- Katherine C. Spelman & James F. Brelsford, *Copyright Issues in Multimedia: Hollywood meets the Internet*, 467 PLI/Pat 189 (1997).

- Barry D. Weiss, *Barbed Wires and Branding in Cyberspace: The Future of Copyright Protection*, 450 PLI/Pat 397 (1996).

- Barbara Cohen, *A Proposed regime for Copyright Protection on the Internet*, 22 Brook. J. Int'l L. 401 (1996).

- Jimenez, *Copyrights On-Line*, 39 How. L.J. 531 (1996).

- R. Timothy Muth, *The Internet's Copyright Web*, 69-OCT Wis. Law. 31 (1996).

- Janice R. Walker, *Protecting Cyberspace: Copyright and the World Wide Web*, 43-MAY Fed. Law. 42 (1996).

- Andrew Grosso, *Copyright and the Internet: A Footnote, a Sleight of Hand, and a Call to Reason*, 44- JAN fed. Law. 44 (1997).

- Ferron, Jr., Christopher J. Daley-Watson and Michael L. Kiklis, *On-Line Copyright Issues, Recent Case Law and Legislative Changes Affecting Internet and Other On-Line Publishers*, 79 J. Pat. & Trademark Off. Soc'y 5 (1997).

Second part: The free use of the Internet thanks to the protection granted by the freedom of speech

- Dominic Andreano, *Cyberspace: How Decent Is the Decency Act?*, 8 St. Thomas L. Rev. 593 (1996).

- Andrew Spett, *A Pig in the Parlor: An Examination of Legislation Directed at Obscenity and Indecency on the Internet*, 26 Golden Gate U.L. Rev. 599 (1996).

- Weiner, *Telecommunications: Internet*, 65 USLW 19 (1996).

- Graham, *Telecommunications: Electronic Mail*, 65 USLW 31 (1997).

- Ellis, *Telecommunications: Internet*, 65 USLE 38 (1997).

- Ellis, *Speech Restrictions on Internet; Communication Decency Act; Minors*, 65 USLW 36 (1997).

- Cabranes, *Telecommunications: Internet*, 65 USLW 6 (1996).

- Dalzell, *Telecommunications: Internet*, 65 USLW 48 (1996).

- Fred H. Cate, *Law in Cyberspace*, 39 How. L.J. 565 (1996).