Crimes in the Internet and how they Influence the Law

Rimal Kawtar Slaoui-Hamda

Lynn University

Follow this and additional works at: https://spiral.lynn.edu/etds

Part of the Science and Technology Law Commons

Recommended Citation
https://spiral.lynn.edu/etds/194

This Thesis is brought to you for free and open access by the Theses and Dissertations Collections at SPIRAL. It has been accepted for inclusion in Student Theses, Dissertations, Portfolios and Projects by an authorized administrator of SPIRAL. For more information, please contact liadarola@lynn.edu.
Slaoui Hamda Rimal Kawtar

GRADUATE PROJECT

CRIMES IN THE INTERNET, 
AND HOW THEY INFLUENCE THE LAW

Submitted to Pr. Snyder

LYNN UNIVERSITY, September 1996.
# TABLE OF CONTENTS

## CHAPTER I : THE PROBLEM AND ITS SETTING

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of the Problem</td>
<td>1</td>
</tr>
<tr>
<td>Subproblems</td>
<td>1</td>
</tr>
<tr>
<td>Hypothesis</td>
<td>2</td>
</tr>
<tr>
<td>Delimitations</td>
<td>2</td>
</tr>
<tr>
<td>Definitions of terms</td>
<td>3</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>5</td>
</tr>
<tr>
<td>Assumptions</td>
<td>6</td>
</tr>
<tr>
<td>Importance of the Study</td>
<td>7</td>
</tr>
</tbody>
</table>

## CHAPTER II : THE REVIEW OF THE RELATED LITERATURE

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>8</td>
</tr>
<tr>
<td>Crimes in the Internet</td>
<td>9</td>
</tr>
<tr>
<td>Laws and Censorship</td>
<td>9</td>
</tr>
<tr>
<td>Internet is International</td>
<td>10</td>
</tr>
</tbody>
</table>

## CHAPTER III : PROCEDURES AND METHODOLOGY

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
</table>

## CHAPTER IV : DISCUSSION

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
</table>

## CHAPTER V : CONCLUSION/RECOMMENDATION

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
</table>

## BIBLIOGRAPHY
CHAPTER I

THE PROBLEM AND ITS SETTING
THE STATEMENT OF THE PROBLEM:

This research proposes to identify and evaluate the crimes perpetuated in the Internet, and how they influence the law.

THE SUBPROBLEMS:

_The first subproblem:_

The first subproblem is to determine if the crimes in the Internet can be diminished and how to reduce them.

_The second subproblem:_

The second subproblem is to analyze if censorship and related regulations fight against crimes on the Internet and whether or not this is a civil liberties issue.
The third subproblem: The third subproblem is to evaluate situations where Americans can be victimized by information from people sitting at computers in foreign lands beyond the reach of The United States authorities.

THE HYPOTHESIS

The first hypothesis is that crimes in the Internet can be reduced through different laws and regulations.

The second hypothesis is that if the Internet is regulated, it would be against freedom of speech.

The third hypothesis is that an International law would be able to regulate the Internet worldwide without having problems of jurisdictions.

THE DELIMITATIONS

The study will not attempt to define the laws and regulations to prevent crimes in the Internet; only how these alleged crimes can be stopped.

The study will not evaluate the feasibility of an International law regarding the prevention of crimes in the Internet.
The study will not attempt to predict the success of an International law regarding the reduction of crimes in the Internet.

The study will not take into account the barriers of the different languages in the Internet.

The study will be limited to the point of view of Americans.

THE DEFINITIONS OF TERMS:

1- **Network**: A number of computers linked together so that they can share information.

2- **Internet**: A global network of thousands of smaller networks, linked together so they can share information.

3- **World Wide Web**: A new Internet feature that offers the same information but makes it look a lot nicer. It takes a special phone hookup to access the graphic part of the Web.
4- **Usenet**: Discussion groups on the Internet, where users can post or download text files and images. Each news group is devoted to a particular subject, from gardening to O.J. Simpson to bestiality.

5- **Surfing**: The act of skimming through the Internet, following trains of thought from one network to another.

6- **E-Mail**: Electronic mail sent by computer and received by computer.

7- **Chat**: A feature that lets people "talk" to each other by exchanging typed messages in real time. The Internet chat feature is called Internet Relay Chat. Like Usenet news groups, IRC sites are devoted to specific topics.

8- **Information Superhighway**: A Clinton administration buzzword for the convergence of communications technology. It includes not only the Internet but also telephone communications and cable television.

9- **Anonymous remailer**: A computer that takes e-mail messages, strips the identifying names and sends them on their way.

10- **Hacker**: A highly skilled computer user; a programmer who delights in going to forbidden places and knowledge.
11- **Cracker**: A hacker gone bad, a cybervandal who uses his skills to break into other computer systems to cause damage or commit crimes.

12- **Encryption**: An e-mail message, usually personally insulting and full of invective. Volleys of this sort, known as flame wars, tend to erupt easily, sometimes over very little--mistakes in grammar, for example--burn brightly for a time, and then die out. It can be unsettling to be flamed, but it is one way norms are enforced on the Internet.

13- **Spamming**: The act of flooding the net, sending the same message to hundreds or thousands of discussion groups. It is considered an inappropriate form of online behavior.

14- **Telnet**: a tool that allows users to log on a remote computer, access files and even run programs.

**ABBREVIATIONS**:

- WWW is the abbreviation used for the World Wide Web.
- LANs is the abbreviation used for Local Area Networks.
- FLETC is the abbreviation used for Federal Law Enforcement Training Center.

- BBSs is the abbreviation used for Bulletin Board Systems.

ASSUMPTIONS:

*The first assumption*: No one owns the Internet, or controls it.

*The second assumption*: More and more people are using the Internet, and more and more criminals are entering it.

*The third assumption*: The Internet allows users expand their horizon without leaving their home, while at the same time limiting personal privacy.

*The fourth assumption*: The United States law does not recognize any right of control over information about individuals.

*The fifth assumption*: The Internet gives people power to literally disappear in cyberspace.

*The sixth assumption*: In this global electronic age, the flow of information is becoming increasingly difficult.
THE IMPORTANCE OF THE STUDY:

The Internet, a global network of interlinked computers, has given individuals the power to obtain information on virtually any subject from all over the world. It has also put into their hands the ability to communicate any message, almost instantly at an extremely low cost, to a potential audience of millions. The number of users is growing at a phenomenal rate. Further, the technology exists and is used today to allow these communications to be anonymous or private and readable only by the intended recipients. The possible consequences of the technology of computer networking worries many people. Anonymous and private communication can be used by terrorists, drug smugglers, and child pornographers, which the United States government offers as argument in attempting to justify restrictions on the use and export of encryption technology.
CHAPTER II

THE REVIEW OF THE RELATED LITERATURE
Statement of the problem:

This research proposes to identify and evaluate the crimes perpetuated in the Internet, and how they influence the law.

INTRODUCTION

A few years ago, the Internet was just an experimental collaboration of the United States Defense Department and the United States academia. But it grew logarithmically as users all over the world discovered the advantages of linking their computers together to share software, exchange electronic mail, and discuss complicated scientific problems. But as more individuals are using the Internet, more crimes are being perpetuated.
CRIMES IN THE INTERNET

The vast majority of the use of the Internet is totally and completely legitimate. Like any community, there is a small percentage of people who are criminals. But as there are more and more people entering the Internet, there are also more and more people that are criminals hooked in it. Most of the criminals are people who simply love to play with the computers. They may break security measures in a net-work, but they do it just for fun, or because they think the flaws need to be pointed out.

LAWS AND CENSORSHIP

A local American Civil Liberties Union official says legislation that seeks to halt “lewd and lascivious” computer messages tramples on First Amendment rights. The Communications Decency Amendment to the Telecommunications Reform Bill, taken into consideration by the Congress, would impose a $100,000 fine or a two year jail term to anyone using computer to “annoy, abuse, threaten, or harass”.
The amendment was proposed by Senator Jim Exon, and a similar bill has been introduced in the House by Representative Tim Johnson. Exon has said the bill is necessary to “extend standards of decency that have protected telephone users to new telecommunications devices.” The proposal was prompted by complaints about the explicit sexual content of some computer bulletin boards, but appears to have more far-reaching implications, according to an alert put out late last week by the Electronic Frontier Foundation.

The foundation, a non profit, computer civil liberties group, says that the amendment tries to apply to on-line media many restrictions that do not apply to printed material. For example, transmitting an on-line version of a “laviscious” book could subject the sender to fines and imprisonment, while mailing the book in hard copy would be protected under the First Amendment.

INTERNET IS INTERNATIONAL

The Internet has stretched the concept of what the law means, where it applies and to whom it applies. Copyright law, privacy law, and the law against spreading hate . . ., all are running up against the technology of the Internet.
As messages on the Internet are passed from computer system to computer system in milliseconds, it crosses border in less time than it takes to cross most streets; the Internet has no frontiers. One of the real problems with the law of the Internet is deciding where the offense occur. Much of what transpires on the Internet is International, so it is very tough to control and to regulate.
CHAPTER III

PROCEDURES AND METHODOLOGY
PROCEDURES AND METHODOLOGY

The statement of the problem:

This research proposes to identify and evaluate the crimes perpetuated in the Internet, and how they influence the law.

THE DATA

The data used for this research is of one kind: secondary data.

The studies and texts dealing with the crimes in the Internet and how they influence the law, as well as management and laws books are the type of secondary data that was needed for this research.

THE CRITERIA OF ADMISSIBILITY OF THE DATA

Only published texts and studies will be used in the study.
The secondary data on the subject of the Internet has been edited to include only the most recent information. Anything printed later than eighteen months ago has been eliminated from this study.

THE RESEARCH METHODOLOGY

The data gathered for this research would be classified in order to come up with a descriptive self-report study.
CHAPTER IV

DISCUSSION
DISCUSSION

Statement of the Problem:

This research proposes to identify and evaluate the crimes perpetuated in the Internet and how they influence the law.

INTRODUCTION

Back in the mid-1960s, at the height of the cold war, the Department of Defense faced a tough question: How could orders be issued to the armed forces if the U.S. were ravaged by a nuclear assault? The communication hubs in place at the time (the telephone, the radio and the TV broadcast) were not only vulnerable to attack, they would also probably be the first to go. The Pentagon needed a military command and control system that would continue to operate even if most of the phone lines were in tatters and the switches had melted down.

In 1964, a researcher at the Rand Corp. Named Paul Baran came up with a solution. He designed a computer-communications network that had no hub, no central switching, no
governing authority, and that assumed that the links connecting any city to any other were totally unreliable. In Baran’s scheme, each message was cut into tiny strips and stuffed into electronic envelopes, called packets, each marked with the address of the sender and the intended receiver. The packets were then released into the web of interconnected computers, where they were tossed back and forth over high-speed wires in the general direction of their destination and reassembled when they finally got there. If any packets were missing or mangled, they were simply re-sent.

Baran’s packet-switching network, as it came to be called, might have been a minor footnote in cold war history were it not for one contingency: it took root in the computers that began showing up in universities and government research laboratories in the late 1960s and early 1970s and became the technological underpinning of the Internet.¹

Nowadays, the Internet is the place to be. College students are queuing up outside computing centers to get on-line. Executives are ordering new business cards that show

off their Internet addresses. Millions of people around the world are logging on to tap into libraries, call up satellite weather photos, download free computer programs and participate in discussion groups with everyone, from lawyers to physicists to sadomasochists.

The Internet is a family place. It is a place for perverts. It is everything rolled into one. As traffic swells, the Internet is beginning to suffer the problems of any heavily traveled highway, including the vandalism, break-ins, and traffic jams. And while most users wait patiently for the access and information they need, rogue hackers use stolen passwords to roam the network, exploring forbidden computers and reading people's mail.

1 - THE CRIMES THAT AFFECT THE INTERNET

No one knows exactly how many computer crimes there really are, though FLETC's experts agree that the damage starts in the billions of dollars and will surely surge upward. The size and scope of cybercrimes are limited only by the bad guys'
imagination, technical skill and gall. But here are the crimes that worry the authorities the most:²

- **White-collar crimes**: Virtually every white-collar crime has a computer or telecommunication link. Sometimes the crimes are simples, such as the case of the bookkeeper at a store who frequently enters incoming checks as returned merchandise, then cashed the checks. Even more damaging are the ones involving skilled computerists.

- **Theft**: Given the expanse of the computer networks, even seemingly small crimes can have big payoffs. "Salami slicing", for example, involves a thief who regularly makes electronic transfers of small change from thousands of accounts to his own. A more targeted approach involves pilfering industrial secrets.

- **Stolen Services**: Swiping and reselling long-distance calling codes is a big business, as is breaking into private phone networks and selling long-distance access.

---

- Smuggling: Drug dealers launder their proceeds through cyberspace and use the Internet to relay messages. Moreover, they cover up secret communications by cracking into corporate voice-mail systems and by operating their own cellular-telephone networks.

- Terrorism: Since computers are the nerve centers of the world’s financial transactions and communications systems, there are any number of nightmarish possibilities. Authorities especially worry that a cracker might penetrate FedWire, the Federal Reserve’s electronic funds-transfer system, or vital telephone switching stations.

- Pornography: Cyberporn is nothing new, it flourished during the 1980s through the popularity of bulletin board systems, or BBSes, locally operated databases nodes that often offered pornography and erotic chat. But with the increasing allure of the Internet, with more than 30 million users, computer porn has taken off. In 1994, a U.S. survey showed that more than 450,000 pornographic images and text files were available to Internet users around the world; that material had been accessed more than six million times. Of particular concern to the forces of law is the presence of child pornography. And there is a lot of child pornography out there.
To combat current and future cybercrimes, FLETC’s Financial Fraud Institute conducts some 14 programs, regularly updated to keep pace with the crimes. Agents learn how to analyze evidence, track credit card fraud and apply constitutional search and seize techniques when they find evidence of crimes on computer bulletin boards systems, or BBSs. This is a new world for law enforcement, because cops have always followed a paper trail, and now there may not be one.

When they start rooting around for crime, new cybercops are entering a pretty unfriendly environment. Cyberspace, especially the Internet, is full of those who embrace a frontier culture that is hostile to authority and fearful that any intrusions of police or government will destroy their self-regulating world. The clash between the subculture of computerists and cops often stems for law enforcement’s inexperience. The Internet buzzes with stories of cops who “arrest the equipment” by barging into BBS operations to haul off all the electronic gear, as if the machines possessed criminal minds.
Still, keeping up with the wise guys in cyberspace will tax the imaginations and budgets of law enforcement agencies and put revolutionary pressures on America’s notions of privacy, property and the limits of free speech.

*Invasions of Privacy*

*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ... The American Constitution, Fourth Amendment.*

Almost anybody with a computer, modem and telephone can surf through cyberspace into the deepest recesses of your private life. A fairly accurate profile of your financial status, tastes and credit history can be gleaned from such disparate things as your ZIP code, Social Security number and records of credit cards usage.

Even more personal information will be available as commercial transactions increase through on-line services. And that raises the most pressing cyberspace issues for everyday Americans. But legal access to data is only one part of the problem. Another difficulty is unauthorized peeking into personal records. The problem is that wrong and harmful “facts” can creep into the databases. In this environment, it is inevitable that Americans will demand stronger privacy protections. The United States has a law
banning the release of video rental records but no strong laws against scanning personal medical data.

**Encrypting Data**

Cybercops especially worry that outlaws are now able to use powerful cryptography to send and receive uncrackable secret communications. That would make some investigations impossible and create a breed of “cryptocriminals”. But there is widespread agreement across the Internet and among entrepreneurs to do business in cyberspace that cryptography is necessary for privacy in a network universe.³

Besides business, which will need cryptography for transmitting sensitive information, the other market for cryptography is the millions who use the electronic mail. Without encryption, E-mail is no more secure than a postcard.⁴

---


⁴ Ibid.
Law enforcers are also deeply worried about another aspect of cyberspace that offers absolute anonymity to anyone who wants it. Anonymous re-mailers can convert return addresses to pseudonyms and render E-mail untraceable.

Cryptography will become even more popular once cybersurfers discover digital cash, which is the electronic equivalent of real money that resides in a computer. Anybody can use it to transfer money for legal or illegal purposes. Many people believe that the widespread use of E-cash will be one more aspect of the Internet that erodes the power of central government.

2 - THE CONTROVERSY BETWEEN LAWS AND REGULATIONS FOR THE INTERNET AND THE FREEDOM OF SPEECH

The advent of space-age telecommunications raises enormous questions about the future of government regulation of media. Though the First Amendment of the American Constitution asserts there should be no law abridging freedom of speech or the press, there have been laws aplenty in the last three generations that regulate speech on new kinds of technology. Different restrictions apply to telephones, radio, TV stations
and cable TV. But cyberspace is a convergence of media and the blurring of distinctions between transmissions modes.\(^5\)

Washington, December 6, 1996: A House - Senate conference committee agreed in principle on tough new prohibitions against transmitting obscenity and "indecent" material over computer networks, rejecting a compromise offered by moderate Republicans and the on-line computer industry. House members of the conference voted 17-to-16 for a measure that would impose fines of up to $100,000 and prison of up to five years for people who make "indecent" material available to minors. However, in deference to on-line services and other electronic publishers, both bills protect companies from penalties if they make "good faith" efforts to keep indecent material out of the hands of minors.\(^6\) The vote means that both the House and Senate support similar prohibitions, the first that would ever be imposed on communications in cyberspace.\(^7\)


\(^6\) Ibid.

\(^7\) Ibid.
The move was immediately denounced by a wide range of civil rights groups, who said the measure would violate constitutional rights to free speech and vowed to challenge it in court. It was also a blow to commercial on-line services and information providers, many of which worry about being embroiled in legal battles over foul language and even for discussions about subject like AIDS.

The key decision was to push ahead with restrictions against providing “indecent” material to people under the age of 18. “Indecency” remains a vague legal concept that falls short of explicit or graphic sexual material but covers four-letter words and sexual material deemed to be patently offensive by local community standards.

Opponents of this restriction argued that the indecency standard is too vague to be constitutional and has been applied only to television and radio broadcasting. The standard has not been used to regulate printed publications, and the new bill raises the incongruous possibility that newspapers would be able to print some words on paper but not in their on-line editions distributed over the Internet.

---


9 Ibid.
The American Civil Liberties Union immediately announced that it would challenge the bill in court if it becomes law, saying it violates the First Amendment rights to free speech.\textsuperscript{10,11}

\textit{Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.} The American Constitution, First Amendment.

\section*{3 - THE INTERNATIONAL PROBLEM OF THE INTERNET}

Modern telecommunications know no borders and has few limits. The liberating potential of the technology is exhilarating. It unleashes information and breaks down communications hierarchies. There is a free flow of information in all directions to all persons who seek it. But it also creates a situation where Americans can be offended or


otherwise victimized by information from people sitting at computers in foreign lands beyond the reach of U.S. authorities.

The saying on the Internet is that bits have no boundaries, and that is equally true of smut. Pornography might be sent from a computer in the United States to a computer in Canada to a computer in Europe, where it may reside, perfectly within the laws of that country. The American police forces can ask for help from other countries, but may not get it. A case may not be a priority, especially if the alleged crime is not illegal in that country. International investigations do not move quickly, and as small countries have sometimes set themselves up as money-laundering havens, others could find it profitable to become data havens. The problems are pushing governments to talk about international treaties governing data flows, but so far little has been done. It is the Net's very lack of frontiers that make law enforcement so difficult. One real problem with the law of the Internet is deciding, where the offence occur.
CHAPTER V

CONCLUSION/RECOMMENDATION
CONCLUSION/RECOMMENDATIONS

Statement of the problem:
This research proposes to identify and evaluate the crimes perpetuated in the Internet, and how they influence the law.

CONCLUSION/RECOMMENDATION

The Dark Side of the Internet, from hate messages to stealing information, is prompting calls for censorship and regulation. Although the Internet has much to recommend it, the dark side of the Internet has people worried. There have been calls for laws to regulate and censor what moves across it wires. Most of the debate about the Internet arises because it is so new. But the debate is actually age-old and boils downs to
what the limits that society sets on free expression. In fact, it is not a computing issue but it is a civil liberties issue.

Freedom of expression is enshrined in the First Amendment of the American Constitution, and the courts have generally protected it from the government encroachment. In many ways, the ethics issues in cyberspace mirror those in the real world. After all, any advance in technology stretches current ethical boundaries. The introduction of the telephone in the last century generated fierce debate about the propriety of ringing up someone without an appointment. But there are profound differences. First, on the Internet, there are no fences, no geography other than an addressing system, no authorities with jurisdiction beyond their own systems. Also, any attempt to set moral standards quickly runs up against the question: Whose standards? Every country has its own standards and it is hard to agree on which ones to chose. Internet service providers can and do establish rules, such as banning advertising, and customers who violate them can be unplugged. But all anyone has to do is sign with another service.

In this global electronic age, meaningfully restricting the flow of information is becoming increasingly difficult, especially as the Internet is international and has no
boundaries. So, it is believed that cyberspace will transcend national borders, national cultures and national economies. Also, it is believed that no one will hold sovereignty over this new realm because force is impotent in cyberspace.

Confronted with the difficulty of trying to grab on to something as amorphous as the Net, some critics and government officials are hoping that the Internet service providers, for a fee, will hook up the companies and individuals, can police the Internet themselves. The information council is expected to approve a recommendation that would encourage the providers to develop a code of ethics, in the same way that the broadcasters have been encouraged to regulate themselves in the transmission of violent television programs. The Internet providers say they cannot hope to control what floods over their networks and trust that they will eventually be considered common carriers, as the telephone companies are, freed from liability for what people say and do over the phone. A United States decision, however, suggests that as long as on-line services do
not provide content, they may not be liable for the information they carry; in other words, they would be treated as a library or a bookstore, not a publisher.

A legislation for the Internet would be hard and mechanically impossible to establish, because of much of what transpires on the Net is international. It is very tough to control and to regulate.
BIBLIOGRAPHY


