

tree

(.pdf)

: (PROV) MAJOR
redistribution
with credit

~~MAKING~~
~~PAPER~~

~~ALLEN ANGEL~~

~~RATED: MVA~~

• This is a selection of
"low bidding" papers from
college (undergraduate)
(so yes, no ~~graduate~~
contingency!) → Redigto
however ~~wysiyg~~ do not
"steal" in any way!!

(Answers!)

A-

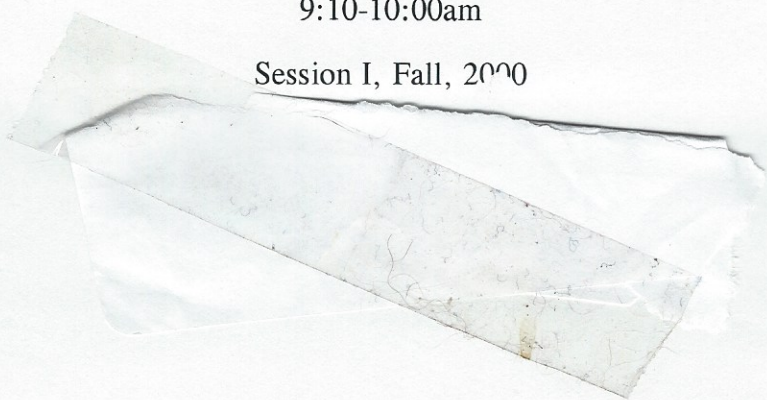
"Censorship On The Internet"

Lee Lee Atkins

POS 2041 - Section 4237

9:10-10:00am

Session I, Fall, 2000



As the technological age rages, it seems as though every family's tapping in, logging on and getting connected to the Internet. The Internet is a network of computers that spans over the entire world compiled of millions of web sites, chat networks, an avid flow of electronic mail, and many other forces. It seems as though these days one can not survive without an email address and a search engine. There has been an ongoing struggle between critics and advocates alike in regards to whether or not there should be some sort of censorship of regulation on the 'net. Here I'm going to shine some light on some of the measures that have been taken by government to do so, what the results were and my opinion on what could happen hereafter.

In 1996 congress passed the Telecommunications Reform Act (TRA) which was signed by President Clinton even though he expressed some reservations about the constitutionality of the Act. (L. Sabato, K. O'Connor, Pg 151) The Communications Decency Act (CDA) is a section of the TRA which states that anyone over 18 who uses an interactive computer service to transmit pornographic material to a minor will be prosecuted. (SEC 502. CDA.) On June 26th 1997 the Supreme Court Ruled the CDA was unconstitutional the majority wrote; "As a matter of constitutional tradition in the absence of evidence to the contrary we presume that Government regulation of speech is more likely to interfere with the free exchange of ideas than to encourage it." (Justice John Paul Stevens.) In 1998 Congress enacted the Child Online Protection Act. (COPA) This act forced commercial web site operators to collect a credit card number as proof of age before allowing access to a site that could be "harmful to minors". Attorney Janet Reno motioned for a restraining order on the COPA which was granted. (Civil Action NO. 98-5591) On February 1st 1999 US district Judge Lowell A Reed Jr. "barred the government from prosecuting anyone under the COPA." (no author found, <http://www.wired.com>) He did however state that "...he would like to see further attempts by Congress to regulate the Net succeed, but the law went too far." (no author

*But it has
been upheld
by the courts
on most
issues*

found, <http://www.wired.com>) The Clinton administration has appealed this decision.
(L. Sabato, K. O'Connor, Pg 151)

The question is: if so far there has been no luck with setting regulations to keep indecent material from our youth what can or should be done? From a personal standpoint; I have been a member of the Internet community for many years, the beginning for me was a local BBS when I was about fourteen, one of about three who were under eighteen on a board full of adults. I was never forced to read anything I didn't want to, and everything I read I chose to read. If anyone goes on the net looking for anything, that's exactly what they are going to find. The chances are slim that they will search for lima beans in an engine and find sites related to hard-core pornography. The youth in question must have seen or heard something related to the subject elsewhere to even know what to look for, this goes back parents and peers. If the net is regulated they will get their hands on the material elsewhere, where there's a will there is always a way. Can the net be regulated? In my opinion the answer is also no, the United States is one of many countries with information on the 'net. No matter what restrictions are placed on it by the US they can't regulate what happens on sites that are run by people in other countries. If I were trying to look at restricted information it would be just as easy to look at an unrestricted site in Sweden as it would be to look at one in the US.

The bottom line is this, censoring the Internet would be a first amendment violation, would be relatively ineffective, and would be impossible to do. The beauty of the 'net is that it is an entire world within a world that gives us the ability to explore outside the limitations of our physical realm. With the freedom to think and feel as we choose there are no regulations, the 'net is made up of the innermost thoughts and feelings of not just the American public, but the entire world. Putting restrictions on that would be like putting restrictions on our minds.

*China is
still
trying -*

BIBLIOGRAPHY.

O' Connor, Karen., and Larry J. Sabato. American Government Continuity And Change. 2000 Edition. Addison Wesley Longman, Inc. 2000

No author reported. "Anti-Smut Law Struck Down." 4:05 p.m. Feb. 1, 1999 PST.
<<http://www.wired.com/news/topstories/0,1287,17664,00.html>. >

United States. Lowell A. Reed, Jr., J Civil Action No. 98-5591 Americal Civil Liberties Union, et. al . V. Janet Reno, in her official capacity as Attorney General Of the United States. District Court For The Eastern District Of Pennsylvania. 1998.

United States. Justice Stevens, John Paul: Writing for the majority. June 26, 1997.
"Supreme Court Rules CDA Unconstitutional." <<http://www.ciec.org/>>

United States. Cong. Senate. Telecommunications Reform Act of 1996,
Communications Decency Act Of 1996 (Computer Section.) SEC. 502. Obscene or Harrasing Use Of Telecommunications Facilities Under The Communications Act Of 1934. Washington D.C. 1996

United States. Office of the Press Secretary. Statement by President Clinton, The White House. June 26, 1996.

Statement by President Clinton

THE WHITE HOUSE

Office of the Press Secretary

June 26, 1996

STATEMENT BY THE PRESIDENT

Today, the Supreme Court ruled that portions of the Communications Decency Act addressing indecency are not constitutional. We will study its opinion closely.

The administration remains firmly committed to the provisions -- both in the CDA and elsewhere in the criminal code -- that prohibit the transmission of obscenity over the Internet and via other media. Similarly, we remain committed to vigorous enforcement of federal prohibitions against transmission of child pornography over the Internet, and another prohibition that makes criminal the use of the Internet by pedophiles to entice children to engage in sexual activity.

The Internet is an incredibly powerful medium for freedom of speech and freedom of expression that should be protected. It is the biggest change in human communications since the printing press, and is being used to educate our children, promote electronic commerce, provide valuable health care information, and allow citizens to keep in touch with their government. But there is material on the Internet that is clearly inappropriate for children. As a parent, I understand the concerns that parents have about their children accessing inappropriate material.

If we are to make the Internet a powerful resource for learning, we must give parents and teachers the tools they need to make the Internet safe for children.

Therefore, in the coming days, I will convene industry leaders and groups representing teachers, parents and librarians. We can and must develop a solution for the Internet that is as powerful for the computer as the v-chip will be for the television, and that protects children in ways that are consistent with America's free speech values. With the right technology and rating systems - we can help ensure that our children don't end up in the red light districts of cyberspace.

-30-30-30-

[Back](#)

Supreme Court Rules CDA Unconstitutional

[Thursday June 26, 1997]

"As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship." -- *Justice John Paul Stevens, writing for the majority*

The Supreme Court today ruled unanimously that the Communications Decency Act violates the First Amendment. Writing for the court, Justice John Paul Stevens held that "the CDA places an unacceptably heavy burden on protected speech" and found that all provisions of the CDA are unconstitutional as they apply to "indecent" or "patently offensive" speech. In a separate concurrence, Chief Justice William Rhenquist and Justice Sandra Day O'Connor agreed that the provisions of the CDA are all unconstitutional except in their narrow application to "communications between an adult and one or more minors."

Source : <http://www.ciec.org/>

Mr. Hartman

ENC1102

“The Rise and Fall of the Condor”

The term “hacker” actually originated as a challenge between programmers, and was coined by programmers at MIT. They would “hack at code” or manipulate their computers to doing exactly what they wanted (Granger 7). Since then the definition has been molded by the public to paint pictures of a malicious person whose only intent is to harm by breaking into secure computer systems. In reality the true definition is a mixture of the two; He or she is not always evil, and is not always attempting the hack with malicious intent. Curiosity brings them to the hack; generally the hacker just wants to solve the mysteries and puzzles generated by software, networks, and the internet. Kevin Mitnick is no stranger to this concept. His assorted past was brought to public attention with the FBI hunt which ended in his 1995 arrest. This paper is an exploration of Mitnick’s criminal history, beginning with his roots as a phreaker, to his most memorable years as a hacker, and finally his newly reformed present.

It all began when Kevin was 13. By this time he was already quite skilled as a ham radio operator. According to Quittner at Time magazine Mitnick had quite a sense of humor. Quittner tells of how Kevin would listen to customers at fast food restaurants as they placed their order then in turn would take control of the drive through’s speaker system and curse the customer for “eating such slop” (Quittner par. 4). His experiences with ham radio were undoubtedly a precursor to the beginning of his hacking career, and

his roots as a phone phreak. A phone phreak is a person who misuses telephone lines in exploration and/or abuse. Since there have been phone lines there have been phone phreaks. In fact hacking is said to have begun with this concept. As there were no computers at the time the curiosity that led phreakers became the same that led, and leads hackers. When telephone networks made the initial transition from analog to digital “skilled manipulators” would dial in and take over the company’s digital central office. This control enabled them to make free long-distance phone calls, listen to other people’s conversations, and perform other phone oriented antics (Freeman par. 8). In 1981 Kevin Mitnick was put on probation for stealing technical manuals from Pacific Bell. Kevin’s intent was undoubtedly to further his knowledge of how the phone system works. (Pennerberg par. 13). This arrest was the first of many to follow thereafter.

Following his arrest in ’81 Mitnick became more adept with systems, programming, and technical skills. As the “Condor” he frequented bulletin board systems (BBS’). On these BBS’ he learned the ins and outs of different operating systems. Learning how to find different exploits and loop holes while bonding with other hacker “associates.” In 1983 he was arrested for breaking into a Pentagon computer from the University of Southern California. For this break in he served six months in juvenile prison (Freeman par. 9). Mitnick again stood before a judge in 1987. This judge ordered him to three years probation for breaking into computers at Santa Cruz Operation the home of a software publication company (Pennerberg par. 13).

In addition, many hackers and phreakers use “social engineering” or “gagging” in order to gain unauthorized access to machines. As described by Mitnick, “Social engineering” is “lying over the phone, coming up with ruses--” in order to pry

information out of people. (Holland par. 11) Mitnick was considered to be a master of social engineering. In fact much of the information Mitnick use to break into systems such as phone numbers, passwords, and ip address came from inside the companies themselves. (Holland, par. 11) Many times Mitnick posed as a co-worker then by using a quick tongue, and an even quicker mind Mitnick managed to talk valuable information out of unsuspecting employees.

Despite previous run ins with the law Mitnick could not kick his hacking habit. Mitnick was arrested again before the capture that led to the demise of his hacking "career". In 1988 Kevin was tried as an adult and convicted as a felon. The judge ordered him to one year in jail and six months in a halfway house where he was to receive treatment for his "addiction" (Sussman par. 4). Eight months of his experience in jail were spent in solitary confinement. Scared officials believed he was able to launch nuclear missiles by simply whistling into a phone. (Pennenberg par. 13).

Once again Mitnick got into trouble. This time he got into trouble by violating his probationary restrictions. In an attempt to prevent further jail time he went "underground"; a term widely used by hackers in hiding. "When the FBI arrived with a search warrant one day to ask whether Mitnick might know, among other things, who was eavesdropping on Pac Bell security officials' voice mail, Mitnick hit the road." (Quittner par. 6). From 1992 till 1995 Mitnick remained on the run. During this time it is said that he used the net to steal software from companies such as Nokia, and Motorola (Freeman par. 11). Perhaps his biggest mistake was breaking into Shimomura's system and downloading software. Tsutomu Shimomura is a computational physicist and security expert who Mitnick had some personal issues with. According to Sussman, a

reporter for U.S. News and World Report, Mitnick had tampered with Shimomura's computer on Christmas day (Sussman par. 6). Taking the attack on his system personally Shimomura led the crusade to apprehend Mitnick. By tracking Mitnick down technologically Shimomura lead the FBI to an apartment in Raleigh, North Carolina ("Infamous" par. 12). At 1:30 am they stormed the apartment and apprehended Mitnick. "The Condor is extinct." was the message received (Sussman par. 1).

Following his 1995 arrest Mitnick spent five years in jail. More than four of the five years he served while still awaiting trial ("Infamous" par. 7). In an interview with Tech TV's Leo LaPorte Mitnick mentions that not only was he held without bail, but did not even receive his right to a bail hearing. During this time Mitnick was tried as a hardened criminal, and as he believes was used as an example. In his words "They wanted to scare the heebie-jeebies out of other computer hackers" (Holland par. 8). In august of '99 Mitnick was "ordered to pay token restitution of \$4125 to companies that had suffered millions of dollars in damage from his exploits ("Noted" par. 1) Mitnick's attorney Donald Randolph asked the court to take the restrictions of electronic usage into consideration. Randolph pointed out the lack of employment opportunity Kevin would have after his release as most business' use computerized items of some sort. Prosecutors had asked that he pay \$1.5 Million" a request which was obviously denied by the Judge ("Noted" par. 5-6).

Naturally, his time was served and Mitnick was freed. Kevin has been on extremely harsh probationary conditions as of January 21st 2000. These conditions include restriction on the use of anything computer related for three years. He may not use cell phones, internet accessible televisions, electronic organizers, and other internet

accessing devices without permission from his probation officer (“Infamous” par. 5).

Mitnick states “I have to live as if I was part of the Amish, and these restrictions even impinge on my freedom of speech: I can’t advise any individual or group that is engaged in computer related activities” (qtd. in Holland, par. 2).

Since his release Mitnick has done many radio, TV, and press interviews. In many cases he advises companies of precautions they can take in order to prevent attacks from hackers. Hopefully Kevin is giving business owners advice that would have protected prior attacks similar to the ones he was accused of. It has been said that many companies are also looking into hiring him on as a security expert. Mitnick believes he would be great for the job stating, “I am a natural in the field of circumventing computer security” (qtd in Holland, par. 6). In December of 2000 Mitnick made national press once more by attempting to auction his prison ID card off on an online auction site. The site refused him permission to do so, but Mitnick argues that he should be entitled. Kevin has stated that he plans to make a living by sharing his knowledge and experience (Freeman par. 17). When he was asked if he believes he was a great hacker Mitnick replied,

I don’t think I was the best hacker in the world. If I had been, I wouldn’t have been caught. There are people out there who have been hacking as long as I was and were never caught. I know of one, I know him by his code name only, who has technical skills far superior to mine and he’s never been caught. If it’s a him; it might be a her (qtd. In Holland par. 12).

In conclusion, some Mitnick supporters believe his only crime was curiosity.

Freeman states, “Mitnick’s actions are very similar to the universal practice of bringing home copies of software from the office, loading them on your home computer, and

returning them the next day” (Freeman par. 12). From his roots as a phreaker, to his focus as a hacker, and finally his self proclaimed reformation Mitnick’s story is an interesting one. As stated by Clifford Stoll, “The term hacker has acquired many meanings, including, a creative programmer, one who illicitly breaks into computers...” to the “Dutch term ‘Computerrendebrenk,’ (literally computer peace disturber)” (Stoll, 494). The true meaning, however, lies with the beholder.

Lee Lee Atkins

Mr. Hartman

ENC1102

Due Date: 10/15/01

Formal Full Sentence Outline.

Thesis Statement: This paper is an exploration of Mitnick's criminal history, beginning with his roots as a phreaker, to his most memorable years as a hacker, and finally his newly reformed present.

I. Kevin Mitnick began his criminal past as a phone phreak.

A. By the age of 13 Kevin had become quite skilled with a ham radio.

1. Had a sense of humor.

2. Would interrupt conversations at fast food restaurants.

B. The ham radio was a precursor to Mitnick's hacking career.

C. Kevin's roots were as a phone phreak.

1. A phone phreak is someone who misuses telephones in exploration and/or abuse.

2. Hacking is said to have begun with phone phreaking.

D. In 1981 Kevin was put on probation.

1. Mitnick was put on probation for stealing technical manuals from Pacific bell.

2. His intent was to further his knowledge of the phone systems.

II. Kevin began to hone his skills as a hacker.

A. As the "Condor" he frequented BBS'.

1. On these BBS' he learned exploits and loop holes.
2. Kevin also used these BBS' to bond with his hacker "Associates"

B. In 1983 Kevin broke into a Pentagon computer.

1. Broke in from University of Southern California.
2. He served six months in juvenile prison.

C. Mitnick was arrested again in 1987.

1. Broke into Santa Cruz Operation (Software Publication Company)
2. He received three years probation.

III. Kevin used social engineering to get information from different companies.

A. Social engineering can be described as:

1. Gaggling.
2. In this context, talking information out of someone by using different manipulative skills. (Smooth Talking?)
3. As described by Kevin "Lying over the phone, coming up with ruses."

B. Kevin was said to be a master of "Social Engineering"

1. Kevin used this skill to talk information out of various employees.
2. The unsuspecting employees gave him valuable information.
 - a. Passwords
 - b. Ip addresses'.
 - c. Phone numbers.

IV. Kevin was arrested in again 1988 before the arrest that led to his demise.

- A. Kevin was tried as an adult and convicted as a felon.
- B. Mitnick was sentenced by the judge to one year in jail and six months in a halfway house for his "addiction".
- C. Eight months out of the year were in solitary because he was believed to be able to launch nuclear missiles by whistling into a phone.

V. Mitnick was finally apprehended by the FBI in 1995.

A. Kevin was underground at this time.

- 1. Underground is another term for going into hiding.
- 2. Kevin went underground in 1992.
- 3. His reasoning for this was because he was questioned on who was eavesdropping on Pac Bell voice mail.
- 4. Mitnick remained on the run until 1995.
- 5. During his time on the run Mitnick attempted to steal software from companies like Nokia and Motorola.

B. Kevin then broke into Tsutomu Shimomura's computer system.

- 1. Shimomura is a computational physicist and a security expert.
- 2. Mitnick tampered with Shimomura's system on Christmas day.
 - a. Shimomura took this attack personally.
 - b. From this time on Shimomura helped the FBI tracking down Mitnick.
- 3. Shimomura led the FBI to an apartment in North Carolina.

C. At 1:30 am they stormed the apartment "The Condor is extinct."

VI. Kevin was arrested, sentenced, and served time.

- A. Mitnick spent five years in jail.
- B. Mitnick served more than four years while still awaiting trial.
- C. Mitnick was held without bail; in fact he didn't even receive a bail hearing.
- D. Mitnick was used as an example to scare other hackers.
- E. In '99 Kevin was ordered to pay restitution of \$4125 for damages.

VII. Mitnick was released January 21st of 2000.

- A. Mitnick was given extremely harsh probationary conditions.
 - 1. Restriction of anything computer related.
 - 2. These restrictions include cell phones, internet accessible telephones, electronic organizers.

B. Mitnick feels as though he is living like the Amish.

VIII. Kevin has done many things since his release.

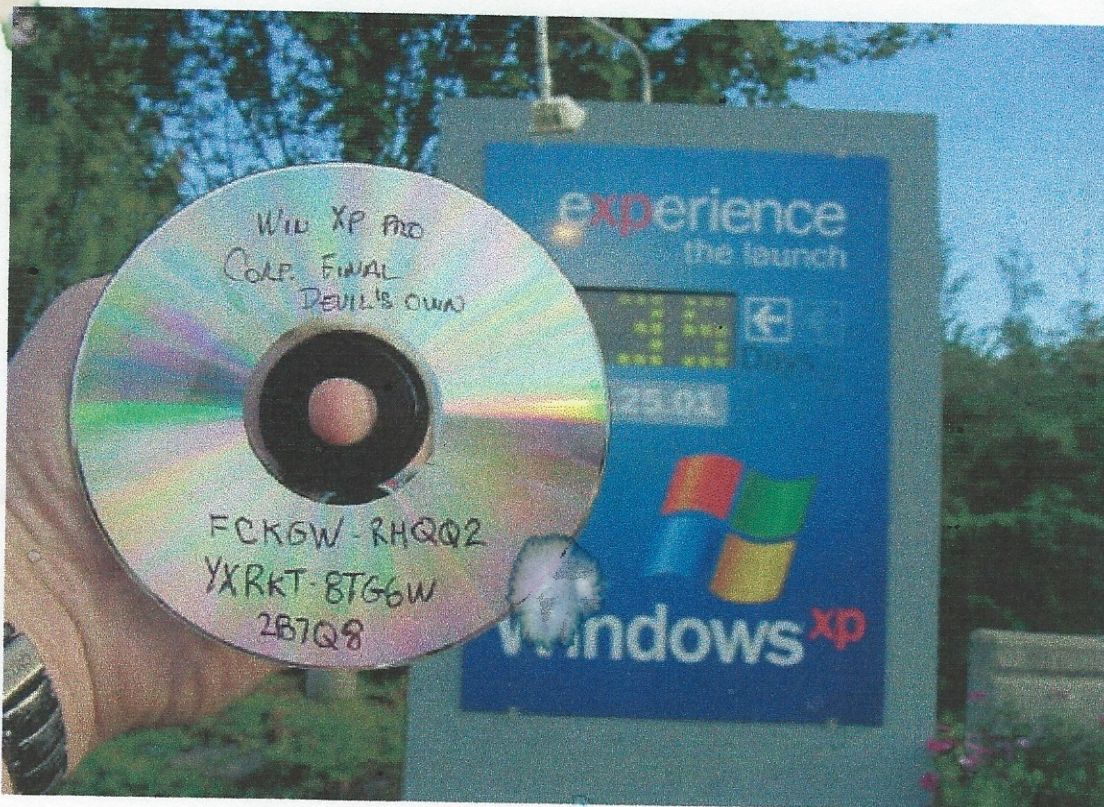
- A. Radio, TV, and press interviews.
- B. Mitnick advises companies on security matters.
- C. It is said that many companies want to offer Mitnick a job as a security expert.
- D. Mitnick tried to auction off his prison ID card on an auction site.
- E. Mitnick plans to make a living by sharing his knowledge and experience.

Name: Lee Lee Atkins
Course: CJE1680 – Internet
Research Paper.

Fighting the Newest Generation of Pirates.

Windows XP, the most recent edition of Microsoft's Windows operating system was scheduled to be released October 25th 2001. This bigger and better version of the windows operating system said goodbye to dos and hello to the promise of its own kernel and a new feel. Windows XP was released with an additional added function which forced users to authorize the software as soon as they began using it. Microsoft attempted regulation by giving users a thirty day grace period in which to activate their software. After the said thirty day period Windows would render itself useless with only the activation option still working...

...On August the 29th of 2001 Windows XP Professional edition was released early by a third party, "Devils Own" all of the activation warnings and nags had been ripped out and the version released was (and still is) fully functional. Microsoft claimed they were releasing hacker proof software, obviously, they were wrong. The Devils Own crew are one of millions who distribute software, music, and other related "should-be-paid-for" media "for free."



“pi·ra·cy Pronunciation Key (pī rə-sē)
n. pl. pi·ra·cies

1.
 - a. Robbery committed at sea.
 - b. A similar act of robbery, as the hijacking of an airplane.
2. The unauthorized use or reproduction of copyrighted or patented material: *software piracy*.
3. The operation of an unlicensed, illegal radio or television station.”
 (<http://www.dictionary.com>)

Piracy is the above mentioned so called “free” distribution of media. Taking software or music which is copyrighted and should be paid for, and using it without paying on an individual basis. The scary fact is that piracy is possible in many forms: Making a taped copy of a neighbor’s CD and listening to it without buying the original is a form of piracy. The copy was acquired without permission; therefore it is considered unauthorized use of copyrighted material. A large percentage of the population has probably committed that very crime and feels absolutely no remorse. This harmless act of buddy swapping probably goes unnoticed as it usually stops there, the chain is broken, and the losses are almost minimal. What if, however, this act is performed on a much larger scale? What if, that copy was given to five friends, and those five friends gave a copy to five of their friends, and so on and so forth? In that case there are copies all over the place and the person who copyrighted the material in the first place could suffer major (financial) loss.

Gallegos states that a software pirate (as copyright law would have it) is anyone who has:

- “given away an old version of software after receiving an upgrade”
- “taken copyrighted software from a server or electronic bulletin board without paying for it”
- “given a copy of proprietary software to a co-worker”
- “‘borrowed’ someone’s software to try it out, then never purchased it”
- “left copies of proprietary software on a hard disk when selling a computer”
- “used shareware without paying the copyright owner for it”
 (Gallegos, par 2.)

It’s difficult for any somewhat “old school” computer user to say they have not done at least one of those things without thinking twice. In the old days of bulletin board systems when the internet was just beginning

the shareware communications software Telex was widely used, this software was almost never paid for as it ran forever even if a registration key was never entered.

According to the Better Business Bureau examples of piracy include softloading, counterfeiting, renting, unbundling, and internet downloading...

Softloading: When software is purchased but used for many computers instead of the amount it is originally licensed for.

An example: Bob buys a copy of Windows XP, and only purchases one copy or one license (gives him the legality to use the program on just one computer) and uses the program on 20 computers throughout the office. Bob is now pirating software.

Counterfeiting: Making, selling, or distributing software which appears to be from the originator or person who owns the copyright.

An Example: Jay takes an original copy of a program and copies it onto another CD then sells it as the original to one of his friends.

Renting: Renting out software for temporary use without authorization from those who own the copyright.

An Example: Tim frequently allows associates to rent his copy of Adobe Photoshop for \$20, his friends then install the software on their computers and use it without buying licenses of their own.

Unbundling: Taking apart software packages which are generally sold together and selling or distributing each piece as separate software.

An Example: Joes computer came with a recovery disk, on that recovery disk were copies of Microsoft Windows, and Microsoft Works. Joe breaks apart the recovery disk and puts Windows and Works on separate CDs; he then uses them separately and gives copies to his friends.

Internet Downloading: Downloading copies of software from the internet and installing them on a computer without purchasing a license for them.

An Example: Pete goes onto Napster and downloads a copy of his favorite game; he then installs the game on his computer and plays it for hours on end without paying for the game at all.

(<http://www.bbb.org/library/pastip.asp>)



Copyrights:

What is a copyright? According to section 102a of title 17 of the United States code (copyright law) "Copyright protection subsides, in accordance with this title, in original works of authorship 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." In other words, when something is copyrighted whether it be music, writing, software, or an idea, the originator (whoever created the song etc.) owns full rights to it.


So what is copyright infringement? Section 501a of the copyright law states "Anyone who violates any of the exclusive rights of the copyright owner provided by sections 106 through 121 or of the author as provided in 106a... ..is an infringer of the copyright of the author, as the case may be." Section 106 gives the illustrates the rights of the copyright owner:

"Subject to sections 107 through 121, the owner of the copyright under this title has the exclusive rights to do any authorize any of the following:

1. To reproduce the copyrighted work in copies or phonorecords.
2. To prepare derivative works based upon the copyrighted work
3. To distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending." (<http://www.copyright.gov/title17/circ92.pdf>)

The Digital Millennium Copyright Act of 1998 outlines a number of rules for electronic media, even though these laws already existed (as above) it was determined that something should be written and put into action to clarify. (<http://www.loc.gov/copyright/legislation/dmca.pdf>)

That means that Making copies, distributing copies, downloading/ uploading copies, hacking code (software code) and altering it, making copyrighted material available for the public and so on and so forth without permission **ARE ALL VIOLATIONS OF COPYRIGHT LAW!**



In the early days of computing software piracy was on a much lighter level than it is now. Usually software didn't go much further than the neighborhood or a few select users of a BBS. Before there were CD-ROMS media had to fit onto floppy disks in order to transfer it, even price could be a factor here; the amount you could steal depended on how many floppies you could afford to buy. Computers were slow, it took a

while to move a file from one place to another, and it's possible you could sit there all day waiting for something to happen. When bulletin boards started to sprout up they were dial up and were usually only local, downloading a file could take days, and if the connection was lost then starting the transfer all over again was almost painful. Piracy did exist but it took work, and knowledge, to pirate software.

Technology feeds its Own Evil.

Computers began to learn, and grow, and change, and become more and more advanced. Hardware and software became bigger, and better, more adaptive, and complex. Users, programmers, and builders became more knowledgeable, and well skilled. As technology grew, so did the ease with which to manipulate it. With the invention of CD burners copies of software became easier to make, and much more reliable. A burned copy of software is an exact replica of the original and will function in the same way. With the new speed of computers, installing software became easier and more convenient. With the cost of parts and utilities becoming cheaper and cheaper it became easier to build bigger, and faster machines to handle piracy related jobs better. The Internet, however, was the missing puzzle piece which gave pirates the one up on manufacturers.

"The Web has increased software piracy..." the Microsoft Anti-Piracy site adds "it's easy for seeming legitimate businesses to create a Web site and then advertise and distribute pirated software. Plus, the explosive growth of e-commerce, combined with anonymity and unlimited volume, have made it even easier for criminals to sell counterfeit software online."
(<http://www.microsoft.com/piracy/basics/what/ip.asp>)

Internet Pirates who surf the web while pilfering and plundering follow after the original Pirates who surfed the seas while doing the same.



With the ability to transfer files at high speeds, and communicate with each other from all over the globe pirates are able to send and receive software at inconceivable rates.

Gallegos agrees, "Internet piracy is on the rise. According to BSA, three major factors are contributing to this rise. The first is the explosive growth in the number of people accessing the internet. At home and at work, the internet is accessed by an estimated 50 million users in the United States alone. Second, the ease of access to the internet has increased along with the advances in technology. Increasingly inexpensive, ever-faster access combined with revolutionary developments in the World Wide Web has allowed pirates to connect with even the most novice of users" (Gallegos, par 60.)



With the inception of the internet various methods began to form which gave pirates the ability to communicate with one another, and transfer files back and forth. Initially it was still quite a challenge to find and distribute files, it still took some work, and much of the time knowing the right people to talk to was a plus.

"Some common vehicles of piracy include:

- Electronic Mail – Pirates can solicit sales of software and attach files to their email messages (eliminating the need to copy programs onto physical media and the necessity of trading in person)
- News Groups/UseNet Services – Can provide a forum in which to transact trades. Software is often broken into pieces and uploaded.
- Internet Relay Chat (IRC) – an interactive (real-time) chat system. IRC chat "channels" (chat rooms) provide a place for pirates to communicate and transfer files between each other directly. The pirates would simply connect with one another and upload/download to each other. (Extremely popular, probably the heaviest medium before the surge of p2p.)
- Mail Order/Auction sites – Believe it or not Pirates are using Auction sites to sell pirated CD's (music and software) and many are selling the same via mail order (usually unsolicited email.)
- File Transfer Protocol (FTP) – These sites permit the exchange of programs and information through uploading and downloading. Using an Internet Protocol Address (a

series of periods and numbers) pirates can log onto one another's computers or often a "dump site" and transfer files. Ftp makes it difficult to catch software pirates."

(<http://www.hawaiianharddrive.com/articleview.cfm?articleid=188> and Gallegos, par 61)

...And then came Peer to Peer (p2p.)...

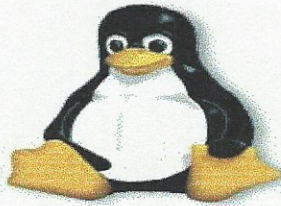
Peer to peer made pirating easy for the beginner. Peer to Peer communication allows clients to communicate directly among themselves. Computers act as both clients, and servers, communicating directly and utilizing various computer resources. Peer to Peer is used for ICQ (<http://www.icq.com>) and various other instant messaging systems. Peer to peer is used in gaming; Doom is an example of a p2p program. Napster, however, is what made p2p famous, and Napster made transferring, searching and receiving software and music simple.

"Internet technology has made copying copyrighted materials much easier. The danger to content owners became apparent in the case of Napster, a service enabling consumers to easily swap compact computer files of copyrighted music via ordinary links to the internet... ..The recording industry Association of America has sued successfully to stop copyright infringement via Napster..." (Munro, par 5.)

Even though Napster has pretty much thrown in the towel, p2p transfer services still exist. They are often taken down, but more seem to rise in their places.



Of course, there are those who believe software should be free. One of these people is Linus Torvalds the creator of Linux, the free (open source) operating system. (<http://linux.com/>)



Linux is also compatible with a large amount of programs; the majority of these are open source also. There are many different Linux distributions (Red Hat, Mandrake...) and each one is also offered for free and can be downloaded from the internet.

Another free option is Freeware. Many people create programs to solve a small program in order to serve themselves, and are quite happy to offer this program to others for free. This is called Freeware. Freeware is all over the internet and can be found with a quick search on Google. (<http://www.google.com>)

Many software companies stopped creating software for fun and started creating it for money. Microsoft is a perfect example, holding place as the richest person in the world for more than seven years according to <http://www.quuxuum.org/~evan/bgnw.html> Bill Gates is worth more than \$34.58 billion dollars, that means he makes at least \$3,924.25 a minute (of course these are just fun estimations, but still!) Each \$199 dollars not spent on his latest operating system is a large dent in the pocket. Its popular belief that as soon as software and music companies figured out how much they were loosing they wanted in. This realization probably caused the recent surge of lawsuits and cases. It is money, after all.

“Bill gates saw it coming early on. In 1976 he was the 20-year-old head of a one-year-old software company when he banged out an ‘open letter to hobbyists.’ ‘Most of you steal your software,’ he fumed. He heaped scorn on the attitude that ‘hardware must be paid for but software is something to share,’ and concluded with a plaintive appeal to ‘anyone who wants to pay up.’” (Stryker, par. 4)

The argument remains, and many still fight for freedom of software. Unfortunately some use that argument as an excuse to pirate software. As they see it: pirating software is harmless, “it should be free anyway...”

“Microsoft won’t say how much money it loses to piracy. But with an 11 percent market share, it’s the largest player in the packaged-software industry, which sells \$175 Billion a year. The industry loses, by conservative estimates, 36 percent of its business to piracy. Microsoft is easily the favorite target” (Stryker, par 5.)

The amount of money lost to piracy each year is phenomenal. The following figures were taken from a “piracy study” which was administered by the Business Software Alliance (BSA):

United States & Canada	1999	2000	2001
Total Piracy Rates	26%	25%	26%
Total Lost Revenue	\$3,631,212	\$2,937,437	\$1,997,008

Western Europe	1999	2000	2001
Piracy Rates	34%	34%	37%
Lost Revenue	\$3,629,371	\$3,079,256	\$2,659,886

Eastern Europe	1999	2000	2001
Piracy Rates	70%	63%	67%
Lost Revenue	\$505,213	\$404,491	\$434,627

The World	1999	2000	2001
Piracy Rates	36%	37%	40%
Lost Revenue	\$12,163,158	\$11,750,365	\$10,967,309

Overall, it seems piracy rates and revenue losses have gone down since the year 1999. However, there is still a long way to go. The entire study can be found at http://www.bsa.org/sweeps/2002_piracyStudy.pdf.

Companies, and the law, are working hard to combat piracy. The fight is ruthless, and piracy (even though it is decreasing,) still exists on major levels throughout the world. There is no telling just how much revenue Microsoft lost to Devils Own or if they are even aware that the crew exists. It is important to educate industry, and computer users on piracy matters so that they have an understanding of the harm piracy really causes. It is easy to be tempted by seemingly "free" music and software but the temptation must be resisted. **The main point is this: as long as companies are allowed to copyright software and sell it, it is illegal to use the same software when not authorized.** Humans almost instinctively know what is morally, and ethically, wrong. Pirated material is **STOLEN**, and stealing is wrong. After a better understanding of what piracy is it is easier to understand why it is so important to fight pirates and reclaim ownership of property. The grueling war on piracy continues but, with the help of computer users, this war can be won.

Works Cited

- Bill Gates Net Worth Page*. August 1 2002.
< <http://www.quuxuum.org/~evan/bgnw.html>>
- Computer Software Piracy*. The Better Business Bureau. 1995-2002.
< <http://www.bbb.org/library/pastip.asp>>
- Copyright Law of the United States of America, and Related Laws Contained in Title 17 of the United States Code*. U.S. Copyright Office, Library of Congress. July 2001.
<<http://www.copyright.gov/title17/circ92.pdf>>
- Gallegos, Frederick., Cindy Cook., "Software Piracy: Some Facts, Figures, and Issues." *Information Systems Security*. Winter 2000. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 28 October 2002.
<<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- Is Software Piracy A Crime or an (Much-Needed) Online-Service* Hawian Hardrive August 2002.
<<http://www.hawaiianharddrive.com/articleview.cfm?articleid=188>>
- McGuire, Stryker., Richard Ernsberger Jr., Tony Emerson., "Software Pirates, Beware." *Newsweek* October 29 2001. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 28 October 2002. <<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- Mearian, Lucas. "Survey: Software Piracy Rates Remain High." *Computer World*. May 28 2001. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 27 October 2002. <<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- Munro, Neil., Drew Clark., "Digital Delemma." *National Journal*. July 28 2001. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 27 October 2002.
<<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- Piracy Basics – What is Piracy*. Microsoft Software Piracy, Protecting Intellectual Property. 2002.
< <http://www.microsoft.com/piracy/basics/what/ip.asp>>

Piracy Study. BSA. June 2002.

<http://www.bsa.org/sweeps/2002_piracyStudy.pdf>

Software and Information Industry Association. 2002.

<<http://www.spa.org/>>

The Digital Millennium Copyright Act of 1998. December 1998.

<<http://www.loc.gov/copyright/legislation/dmca.pdf>>

Name: Lee Lee Atkins
Course: CJE1680 – Internet
Research Paper.

The History of All Things Hacker.

Carrier Detected

2400

Welcome to Protovision Systems, Sunnyvale, CA.

LOGON: *****

Greetings Professor Falken.

Shall We Play A Game?



War Games is probably the most definitive hacker movie, breathing life into technology, and offering the thrill, and excitement which can only be found in the awe of the computer world. In this 1983 movie David Lightman (played by Matthew Broderick) steals passwords to the schools computer system, uses phreaking techniques to make phone calls, and becomes obsessed with finding a "backdoor" to an

unexplainable "logon" prompt. After researching, and finding the information he needs to login to this unfamiliar computer system he is approached as a one "Professor Falken" and is asked "Shall We Play a Game?" Choosing from games such as chess, poker, biochemical warfare, and global thermonuclear war Lightman, (believing he is just playing a game) actually initiates the NORAD countdown to world war three.....In the movie, of course, everything irons itself out and happy endings are in order.

The question is, where did all the terminology come from, the ideas, the thoughts, the actions, who was David Lightman really based on?

And the Answer: On Hackers, crackers, phreaks, and the like, who grow through the ages while leaving behind a piece of cyber history.



In 1876, Alexander Graham Bell had an idea. This idea, rather strange at first, was to make it possible for two people to talk to one another from entirely different places. Getting his invention to work was the first obstacle but after many years, and much money and struggle the patent for the telephone was accepted. Alexander Graham Bell can be accredited with starting the entire hacking revolution. Without the telephone there would never have been phone phreaks, not to mention modems. Thanks Alex!

Of course, with the telephone came the first telephone abusers. Young boys were hired at the time to operate switch boards, and connect calls. Being pranksters these boys often interrupted calls, misdirected calls, and were a general all around nuisance. It has long been considered that those boys were the first phone phreaks as they "cracked" the phone network (at least as far as they could.) The boys were, of course, fired from their positions and entirely new personnel were hired. This time women were used, it was believed that women were

kinder, gentler, and much less likely to begin pulling pranks like the boys did.

(Jargon Dictionary or The New Hackers Dictionary - "a collection of slang terms used by various subcultures of computer hackers. Though some technical material is included for background and flavor, it is not a technical dictionary; what we describe here is the language hackers use among themselves for fun, social communication, and technical debate.")
[\(http://www.tuxedo.org/~esr/jargon/html/\)](http://www.tuxedo.org/~esr/jargon/html/)

Phone Phreak, Phreaker – (If Phone begins with a "PH" it's only logical that in this reference Phreak should begin with one too.)

According to the Jargon Dictionary: A "**phreaker** /freak'r/ n. is One who engages in **phreaking**.

And "Phreaking /freak'ing/ n. [from phone phreak] The art and science of cracking the phone network (so as, for example, to make free long-distance calls).

<http://www.tuxedo.org/~esr/jargon/html/entry/phreaking.html>

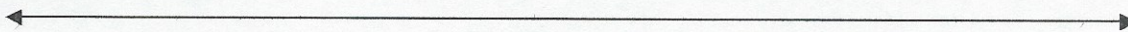
Believe it or not, the first famous phone phreak was a blind student from the University of South Florida. "The Whistler," as he was later nicknamed was a mathematics student from the late 1960's who found out he could make free long-distance calls. "Joe Engressia found he could whistle into a pay telephone the precise pitch – the 2600-cycle note, close to a high A – that would trip phone circuits and allow him to make long-distance calls at no cost." Apparently an operator could tell the difference between the two, but the phone circuits could not. "In 1971 an Esquire magazine article crowned him as one of the granddaddies of telephone hacking, known as "phone phreaking" (Times, par 2-4.)



The most talked about phone phreak is probably John Draper or "Cap'n Crunch," as he was later nicknamed. In 1972 this Vietnam vet was "turned onto a toy whistle" by a blind kid named Denny. "In conjunction with a blue box" it was found that by covering one of the holes and blowing into the whistle, which was found in Cap'n Crunch cereal boxes, that he was also able to fabricate that same 2600 MHz tone and trip the phone circuits to make calls of his own.

(Hansen, par 9 & <http://www.webcrunchers.com/crunch/story.html>)

“Woz” (Steven Wozniak) “begged” Cap’n Crunch to show him how to use a blue box at UC Berkley. Wozniak learned how to make this blue box from information he found in 1971 edition of Esquire magazine. (This article can be found at <http://www.mbay.net/~mpoirier/lbb.html>) Wozniak sold blue boxes for \$150 each “a few months later Intel announced the 8080 Microprocessor chip. Steve Wozniack got his hands on some 6502 chips” using some of the money he made selling blue boxes, and later became the founder of Apple computers with his friend Steve Jobs (<http://www.webcrunchers.com/crunch/story.html>.)



As phone phreaking became more, and more popular, and knowledge was spread about the world, the community began to play with, and learn, the workings of the computer. Armed with 300 baud modems these phreaks began to log on using the phone system to communicate, and share...

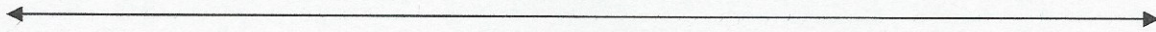
“The beginning of the hacker culture as we know it today can be conveniently dated to 1961” “MIT’s tech Model Railroad Club adopted the machine as their favorite tech-to and invented programming tools, slang, and an entire surrounding culture that is still recognizable with us today.” (<http://www.tuxedo.org/~esr/writings/hacker-history/hacker-history-3.html>, par 1)

When techies, geeks, engineers, and the like began to learn how computers could ultimately change business practices, and lives, forever ARPANET came into the light. Being what was probably the beginning of the internet “ARPANET was the first transcontinental, high speed, computer network.” Built by the defense department, ARPANET became a place for millions to “exchange information with unprecedented speed and flexibility...” “...but the ARPANET did something else as well; its electronic highways brought together hackers all over the U.S. in a critical mass.” (<http://www.tuxedo.org/~esr/writings/hacker-history/hacker-history-3.html>)

It seems that everything began on ARPANET all the first ideas, thoughts, and feelings regarding subjects such as hacker slang, and the hacker ethic (that all information should be open and available to anyone,) were all held on ARPANET. One of the most infamous documents to originate from ARPANET was the Jargon File. (<http://www.tuxedo.org/~esr/jargon/html/>)

Ward Christensen and Randy Seuss created the first BBS (bulletin board system.) CBBS was released in 1978, “making it possible to call

their telephone number with any other computer that had a modem attached, connect to CBBS and post messages.” The BBS system became a central point for hackers and phreaks to meet and share ideas. BBS’s were popular for many years after their inception and the hacker community grew extensively with this computerized meeting place.
[\(http://prehistory.bbsdokumentary.com/\)](http://prehistory.bbsdokumentary.com/)



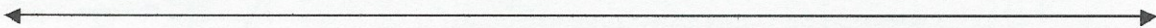
Once the playground had been erected the hackers and phreaks began to play...

The Hacker: - “The entire definition of ‘Hacking’ is somewhat obscure. Hacking originated as a challenge between programmers. Programmers at MIT are known for coining the term. Individuals would ‘hack at code’ meaning that they would work at programming problems until they could manipulate their computers into doing exactly what they wanted”
 (Granger, par 1.)

According to the Jargon Dictionary: **2.** One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. **3.** A person capable of appreciating hack value. **4.** A person who is good at programming quickly. **5.** An expert at a particular program, or one who frequently does work using it or on it; as in ‘a Unix hacker’. (Definitions 1 through 5 are correlated, and people who fit them congregate.) **6.** An expert or enthusiast of any kind. One might be an astronomy hacker, for example. **7.** One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. **8.** *[deprecated]* A malicious meddler who tries to discover sensitive information by poking around. Hence ‘password hacker’, ‘network hacker’. The correct term for this sense is cracker.
[\(http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html\)](http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html)

Knowing that the term “Hacker” is often used in place of “Cracker” leaves room for the understanding that these are two different kinds of people. The Hacker is usually one who does for the common good, often searching for security leaks and exploits within programming, and reporting them to the creator. The Cracker, however, would use those same security leaks to benefit themselves (usually to steal information and/or software.)

When playing there are usually the good guys and the bad guys...



“Cracker” Pat Riddle used the ARPANET to “hack into computers at the Pentagon, the White House, and other high-profile institutions. “Captain Zap” (his handle) “used his PC to pilfer more than \$500,000 in merchandise from several large computer companies.” In 1981, the FBI caught up with Riddle and he was “indicted for stealing property and legal telephone service” (Hansen, par 15-16.)

Once again, there are the good guys and the bad guys, both seem equally famous in their own right. In 1982 “Hacker” Richard Stallman launches the GNU project. The GNU project involved the introduction of a new free clone of UNIX. Stallman grasps the true essence of what being a hacker SHOULD have been about - The hacker ethic - “information should be open and available to everyone.” (<http://www.stallman.org/>)

The infamous movie War Games was released in 1983. This movie probably marked the glorification of what cracking really is. At this point there was much confusion over what the difference between a hacker and a cracker was and the word hacker began to encompass a bad name... ..Interestingly enough Broderick broke into the school’s computer system again in the movie “Ferris Buellers Day Off”. Broderick’s excursions on the big screen made attempting feats like these look “cool.” This look probably sparked more interest in learning how to crack and many teens rushed to their computers to start training. “War Games, portrayed young hackers as high-IQ superheroes” (Wilson, par 2.)

(Note : By this point in history, the term hacking is generally used for both hacking and cracking; for the sake of confusion from now on they both be referred to as Hacking...)

Hacker groups began to form in the 1980’s...

A small group of “high school aged” kids from Milwaukee formed the 414s (named from the area code) in 1984. Using “default passwords” and Telnet, these kids logged onto computers at random. Eventually the 414s hit Sloan-Kettering and Los Alamos, “the damage done by the hackers was reportedly minimal.” It seems that they broke into the computers to prove they could do it. The challenge is very often what draws the hacker to the hack. It’s not so much that they are looking for anything; they just want to be able to brag to their friends about doing it. (http://www.atarimagazines.com/creative/v10n1/266_Telecommunications_talk.php)

The Legion of Doom – Began in the summer of 1984, and has been “enshrouded in secrecy.” According to the Legion of Doom technical journal, “the Legion of Doom will long be remembered in the computer

underground as an innovative and pioneering force, that consistently raised the collective level of knowledge and provided many answers to questions ranging from the workings of the telephone system to the structure of computer operating systems.”

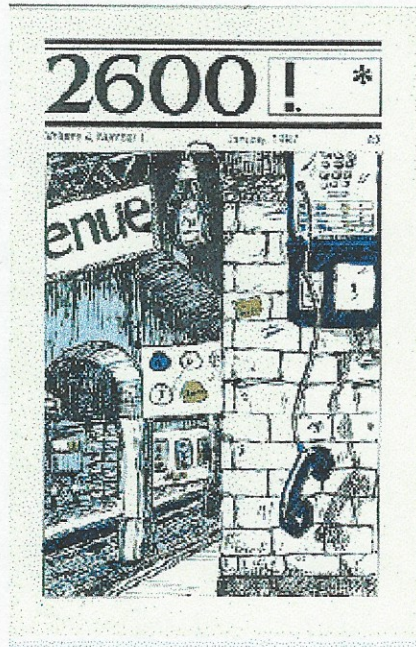
(http://voidspace.hypermart.net/Hacking/legion_journal.html)

When speaking on the Legion of Doom in his book The Hacker Crackdown, Bruce Sterling States: “It wasn’t the crimes they were committing it was the potential hazard, the sheer technical power LoD had accumulated, that had made the situation untenable.”

2600 Magazine was brought into print in 1984. This magazine, named after the 2600 MHz tone used in phone phreaking, became the hacker quarterly. Offering tips, tricks, hints, and secrets related to everything hacker, cracker, and phreaker. 2600 Magazine was followed a year later by the first online h/c/p (hacker/cracker/phreaker) magazine “Phrack.” (Phrack = phreak + hack.) “Usually written by actual hackers. Phrack articles are published in a wide range of styles, ranging from quirky hackerese to the highly technical” (Lange, par 9.)

The 2600 Website (<http://www.2600.org/>)

The Phrack Website (<http://www.phrack.org>)



←—————→

The Computer Fraud and Abuse Act of 1984.

Outlining various fraudulent activities which occur in connection with computers the Computer Fraud and Abuse Act of 1984 was obviously put into place to help stop computer crimes.

The list of Fraudulent behaviors includes anyone who:

“knowingly accesses a computer without authorization or exceeds authorized access”

“intentionally accesses a computer without authorization or exceeds authorized access”

“knowingly and with intent to defraud, accesses a Federal interest computer without authorization”

Basically anyone who accesses any computer without permission, for any reason, is under violation of the law.

(<http://www.cerebalaw.com/cmpfrd.htm>)

The Government Attempts to Crack down On Computer Crime



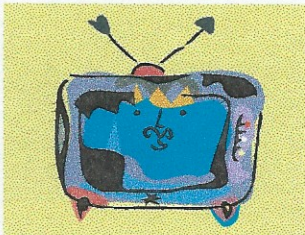
One of the world’s most notorious hackers, Kevin Mitnick (AKA the Condor) was arrested in 1989. Although this was not his first arrest (not his last either) it was a rather severe case. Mitnick was accused of stealing “\$1million dollars worth of software from Digital Equipment Corporation, and the theft of long distance from MCI.” “Mitnick was sentenced to 1 year imprisonment with conditional probation thereafter, stating that he could not use a computer or associate with other computer criminals.”

(<http://www.securitystats.com/crime.asp>)



Also in 1989, members of the above mentioned Legion of Doom are arrested. Franklin Darden (the Leftist), Adam Grant (The

FREE KEVIN



In 1995 the movies Hackers, and The Net are released. In hackers they are in awe over Acid Burn's new laptop with its 28.8 modem. In fact, most of the hardware talked about in Hackers was dated by the time the movie was released...

<http://movieweb.com/movie/hackers/>

By 1996 about 40 million people are connected to the internet...

A huge surge of hacked websites breaks out in 1996, hacked governmental and related sites include;

- CIA (September 19, 1996)
<http://www.2600.com/hackedphiles/cia/>
- Air Force (December 29, 1996)
<http://www.2600.com/hackedphiles/airforce/>
- The Department of Justice (August 17, 1996)
- NASA (March 5, 1997) <http://www.2600.com/hackedphiles/nasa/>
 - (more hacked sites can be found at
http://www.2600.com/hacked_pages/old_archives.html)

In December of 1997, hackers hacked the Yahoo website. "For the past month, anyone who has viewed Yahoo's page and used their search engine, now has a logic bomb/worm implanted deep within their computer," "on Christmas Day, 1998, the logic bomb part of this 'virus' will become active, wreaking havoc upon the entire planet's networks" boasted the website.

"The note said an 'antidote' program will be made available if hacker (yep you guessed it...) Kevin Mitnick is released."

... The threat did, however, turn out to be a hoax. "We immediately took action to see the extent of the damage and moved to correct it," said Diane Hunt, a spokeswoman for Yahoo. "And about that virus? There is,

<http://www.symantec.com/avcenter/warn/backorifice.html>

December 1998, "two hackers who broke into a bank computer network and stole 260,000 Yuan were sentenced to death by a court in eastern China.....the two opened 16 accounts under various names in a branch of the bank in September, and later broke into the branch to install a controlling device in a bank computer terminal. They used the device to electronically wire 720,000 Yuan in non-existent deposits into the bank accounts. Afterwards, they successfully withdrew 260, 000 Yuan from eight different branches of the bank."

http://www.infowar.com/hacker/hack_122998b_j.shtml

...And hackers think the law comes down too hard on them in the states? Tell them to move to China...



Computer viruses become pretty wide spread...

According to the Jargon File – a VIRUS is a cracker program that searches out the other programs and 'infects' them by embedding a copy of itself into them, so that they become Trojan horses. When these programs are executed the embedded virus is executed too, thus propagating the 'infection.' This normally happens invisibly to the user, unlike a worm, a virus cannot infect other computers without assistance. <http://www.tuxedo.org/~esr/jargon/html/entry/virus.html>

In January of 1999 the Happy99.worm is discovered. "When executed," states Symantec "the infected program opens a window entitled "Happy New Year 1999!!" and shows a fireworks display to disguise its installation. This worm sends itself to other users when the infected computer is online."

<http://securityresponse.symantec.com/avcenter/venc/data/happy99.worm.html>

The Melissa Virus: This well known and fast spreading virus was "distributed as an email-attachment that, when opened, disables a number of safeguards in Word 97 or Word 2000, and if the user has the Microsoft Outlook e-mail program, causes the virus to be resent to the

multiplied even faster after the World Wide Web came into play. The years 2000, 2001, and 2002, had an enormous amount of "hacker-related-things" reported.

It would be impossible to name even half of them but here are a few choice highlights...

In January of 2000 Kevin Mitnick is finally released from Jail. After spending five years in prison Mitnick was released "under unprecedented conditions: He cannot touch a computer, or without limitations, a cell phone, or any other device that allows him to get onto the Net." Mitnick did manage to negotiate a deal with his probation officer; he can have a cell phone "as long as the court gets a copy of his monthly phone bill. If the courts determine that Mitnick used the phone to go online, his probation would be considered violated" (Sheff, par 4-5.) Kevin will be completely free in January of 2003 there is a countdown on the "Free Kevin" website at <http://www.freekevin.com>. In a recent interview with Tech TV's Leo Laporte, Kevin states that the first thing he will do when he is free is "go buy the fastest laptop available."

DoS Attacks- Denial of Service.

According to the Jargon File - [Usenet, common; note that it's unrelated to 'DOS' as name of an operating system] Abbreviation for Denial-Of-Service attack. This abbreviation is most often used of attempts to shut down newsgroups with floods of **spam**, or to flood network links with large amounts of traffic, or to flood network links with large amounts of traffic, often by abusing network broadcast addresses.
(<http://www.tuxedo.org/~esr/jargon/html/entry/DoS-attack.html>)

A Large amount of these attacks are reported for the beginning of 2000. The person responsible for the DoS attack just has to take a list of IP numbers from a server, find out where there is a vulnerable computer on the network. Then flood the computer with queries so that it will completely "gum up" the network. Attacks on Yahoo, and other "prominent" including MFN which provides connectivity to eBay. "The person who was instigating (this) attack was amused by his ability to cause eBay to use all it's CPU cycles... when it had no effect, they stopped launching it."
(<http://www.wired.com/news/politics/0,1283,34294-2,00.html>)

DoS attacks are usually administered by "Script Kiddies" - According to the Jargon File Script Kiddies are: The lowest form of **cracker**; script kiddies do mischief with scripts and programs written by others, often without understanding the **exploit** they are using. Used of people with

FBI has announced an ongoing effort to create and deploy best-of-breed electronic surveillance software." "While we applaud the innovation and drive of the federal law enforcement agency, those of us who are US citizens would be remiss if we did not offer our expertise in this area." "There will be absolutely no shared code between the two projects, in order to skirt detection by commercial antivirus packages. The code will remain totally secret. The software will never surface publicly. And it will be far more stealthy than anything we have ever released, demonstrated, or publicly discussed." This new version of Back Orifice will serve as an "artificial witness which is capable of intercepting any and all relevant activity during, after and even leading up to the commission of a computer crime." "The cDc concluded that the project would deliver the 'ultimate intelligence gathering tool. And we intend to construct it, at no cost, exclusively for the use of the federal government" states Flemming. (http://www.infowar.com/hacker/01/hack_121401a.j.shtml)

It will be interesting to see just how many cDc members are brought up on criminal charges, or whether some of their crimes (if there are, of course, any committed) go overlooked. It's hard to believe there won't be a payoff for this somewhere...



A couple of the original hackers, Steven Wozniak and Steven Jobs are working toward a "hack proof Mac." The new OS X operating system is based on the BSD (UNIX) Kernel. "Hackers know far more about" UNIX which causes concern and a need for tougher security. According to an Article in Businessweek online from January 2002 "Apple has made considerable progress." Apple has "created a support team for responding to security questions, or complaints, plus a mailing list for customers who want to keep abreast of the issue." Apple has also "set up a toll-free number for reporting incidents." Salkever gives Apple a "toast for their wise decision to ship OS X with most of the advanced UNIX communications," OS X ships with a "locked down" configuration which "prevents less savvy Mac users from unwittingly exposing their machines to the ne'er do wells cruising the internet." Salkever also mentions OS X's firewall, apparently a more "solid barrier" is in place which keeps OS X much much safer.

(http://www.businessweek.com/technology/content/jan2002/tc20020118_5251.htm)

...And it was only years ago that they were freaking with Cap'n crunch and selling blue boxes at school.....but hey, there would be no Apple if they had not had the blue boxes to sell...





It only seems fitting to end with information taken from an article regarding the increased amount of hack's which have taken place in the world through the year 2002...

According to the BBC (British Broadcasting Company) August of 2002 "set to become the worst year for digital attacks on record." "The total for the first eight months of 2002 reach(es) over 31,000, which is more than the total for the whole of 2001." DK Matai, the chairman of mi2g warns against further "chaos in cyberspace."

"Hack Attacks:

- 1998 - 269
- 1999 - 4,197
- 2000 - 7,821
- 2001 - 31,3222
- 2002 - 45,000+"

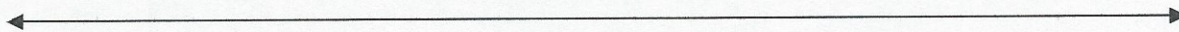
Matai "urges firms, especially those in sensitive industries, to look at detailed personnel vetting and to keep a close eye on voice and data communications."

<http://news.bbc.co.uk/1/hi/technology/2231205.stm>



Through the ages, hackers, crackers, phreakers, and their associates have run rampant through the cyber world leaving little tracks, and sometimes big problems, behind them. Their curiosity has taken them through a universe that can only be understood by a cyber trained mind. While finding loopholes, exploits, and manipulating systems and software, hackers have left many in awe, often leading the way through mazes which are incomprehensible by "just any" mind. The movie War Games might have glorified the hacker culture a little more than it should, but the idea remains the same. Hackers "explore the details of programmable systems" (including the phone and radio) "and how to stretch their capabilities" (Granger, par 2.) Unfortunately there is such a fine line between the good and the bad when it comes to the hacking community. Taking something a little too far can mean instant danger, and run-ins with the law. It is important to document EVERYTHING, and have a clear understanding of what is illegal and what is not...

In the words of Professor Falken's computer, perhaps in the game of hacking, cracking and phreaking, "...the only winning move is... not to play..."



Works Cited

- "BBS Prehistory." *BBS: A Documentary: Prehistory*.
<<http://prehistory.bbsdocumentary.com/>>
- Clark, Donald., "Government Cracks Down On Hacker." *Phrack World News*. <<http://www.phrack.com/phrack/41/P41-12>>
- "Computer Crime – Arrests and Convictions." *Computer Security Statistics*. October 1998.
<<http://www.securitystats.com/crime.asp>>
- "Computer Fraud and Abuse Act." 1993.
<<http://www.cerebalaw.com/cmpfrd.htm>>
- Draper, John T., "Cap'n Crunch in Cyberspace." *John T Draper (AKA Captain Crunch)*. 2001.
<<http://www.webcrunchers.com/crunch/>>
- "Florida's Hacker Connections." *The St Petersburg Times ONLINE*. 2002.
<<http://www.sptimes.com/Hackers/florida.hackers.html>>
- "Free Kevin Mitnick.," *The Official Kevin Mitnick Site*.
<<http://www.freekevin.com/>>
- Granger, Sarah., "The Hacker Ethic." *Association for Computing Machinery*. January 1994. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 26 October 2002. <<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- "Hack Attacks On The Rise." *BBC News*. Sept. 2002.
<<http://news.bbc.co.uk/1/hi/technology/2231205.stm>>
- "Hackers." *Movie Web*. 2002. <http://movieweb.com/movie/hackers/>
- "Hacked Sites (Who Have They Hacked Now.)" *2600 Magazine*.
<http://www.2600.com/hacked_pages/old_archives.html>
- Hansen, Brian., "Early Hackers Wanted to Advance Technology, not Deminish it." *CQ Weekly*. June 2002. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 24 October 2002. <<http://www.spcollege.edu/central/libonline/resources/index.htm>>.

- “Information on Back Orifice and NetBus.” *Symantec – Security Updates*. 2002.
<<http://www.symantec.com/avcenter/warn/backorifice.html>>
- “Infowar – It All Starts Here.” 2002. <<http://www.infowar.com/>>
- Komando, Kim., “Hackers and Crackers.” *Popular Mechanics*. April 1999. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 28 October 2002. <<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- Kuehl, Daniel T., “Masters of Deception: The Gang that Ruled Cyberspace.” *Air and Space Power Chronicles*. <<http://www.airpower.maxwell.af.mil/airchronicles/bookrev/slatta.html>>
- Lange, Larry., “Phrack’ Aims To Clue In the Suits.” *Electronic Engineering Times*. January 1996. *Achademic Search FullTEXT Elite*. EBSCOHOST. M.M.Bennett Lib., St Petersburg College. 28 October 2002. <<http://www.spcollege.edu/central/libonline/resources/index.htm>>.
- “Legion of Doom Technical Journal.” *LOD Technical Journal*. June 1993. <http://voidspace.hypermart.net/Hacking/legion_journal.html>
- McCullagh, Declan., “Sleuthing Out the DoS Attacks.” *Wired News*. Feb 2000. <<http://www.wired.com/news/politics/0,1283,34294-2,00.html>>
- “Melissa Virus.” *SearchSecurity*. July 2001. <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213491,00.html>
- “News Archive.” *Project Gamma*. Various Dates. <<http://www.projectgamma.com/news/archive/index.shtml>>
- “The Jargon File.” *The New Hacker’s Dictionary*. Sept 2002. <<http://www.tuxedo.org/~esr/jargon/html/>>
- “Richard Stallman’s Personal Home Page.” *Richard Stallman’s Personal Home Page*. 2002. <<http://www.stallman.org/>>
- Rosenbaum, Ron., “Secrets of the Little Blue Box” *Esquire Magazine*. Oct 1971. <<http://www.mbay.net/~mpoirier/lbb.html>>

Sandoval, Greg., "eBay Sells for \$1.25 in Bogus Auction." *c|net news*.
Sept 1999. <<http://news.com.com/2100-1023-260557.html?legacy=cnet&tag=st.ne.1002.thed.1007-200-123220>>

Salkever, Alex., "Toward A Hack-Proof Mac." *BusinessWeek Online*.
Jan 2002.
<http://www.businessweek.com/technology/content/jan2002/tc20020118_5251.htm>

Sheff, David., "Free Kevin Mitnick!" *Yahoo Internet Life*. October 2000.
Achademic Search FullTEXT Elite. EBSCOHOST. M.M.Bennett
Lib., St Petersburg College. 28 October 2002.
<<http://www.spcollege.edu/central/libonline/resources/index.htm>>.

"Telecommunications Talk." *Creative Computing*. January 1984.
<http://www.atarimagazines.com/creative/v10n1/266_Telecommunications_talk.php>

"The Early Years." *A Brief History of Hackerdom*. 2002.
<<http://www.tuxedo.org/~esr/writings/hacker-history/hacker-history-3.html>>

"The history of the Web Beginning at CERN." *History of the Web Beginning at CERN*. June 2002.
<http://www.hitmill.com/internet/web_history.asp>

in crossing:

"It is the only
design, the

way it is used

in the original

~~Basic~~ elemental
design."

where
used
element